Regulating hosting ISPs' responsibilities for copyright infringement

Regulating Hosting ISPs' Responsibilities for Copyright Infringement

The Freedom to Operate in the US, EU and China

Dissertation

to obtain the degree of Doctor
at Maastricht University,
on the authority of the Rector Magnificus,
Prof. dr. Rianne Letschert
In accordance with the decision of the Board of Deans,
to be defended in public
on 12 October 2016, at 14:00 hrs

by

Jie Wang

Supervisor:
Prof. Anselm Kamperman Sanders
Co-supervisor:
Dr. Ana Ramalho

Assessment Committee:
Prof.dr. Sjef van Erp (Maastricht University) (chair)
Prof.dr. Dick van Engelen (Maastricht University)
Prof.dr. Estelle Derclaye (University of Nottingham)
Prof.dr. Meir Pugatch (Maastricht University)
Prof.dr. Peter Ganea (Tongji University)

Table of Contents

Acknowledgements

Acknowledgements

Five years ago, I got on the airplane from Shanghai to Amsterdam, and started my PhD life in a lovely city, Maastricht. Five years might be just a small piece of one' life, but this five years are very special to me and leads me to the next step in my life. On the way of accomplishing a PhD in law, I was lucky enough to receive so much support from numerous colleagues, friends and family.

I am forever indebted to my supervisor Prof. Anselm Kamperman Sanders. Without his support, I would never come to Maastricht University to start my PhD, and without his supervision, it would be impossible for me to finish my PhD. The same gratitude must be also given to my co-supervisor Dr. Ana Ramalho who stepped into the supervision at the final stage of my writing, and provided me lots of insightful comments on my manuscript. Without her help, it might take me more time to finish a PhD thesis qualified for defense. I feel owed to Prof. Kaizhong Hu, my supervisor in China. Although after I came to the Netherlands, he was officially not my supervisor anymore, he still continuously delivered his support to me. I also would like to thank my colleagues in the Faculty of Law, Dr. Cornelis Antonius Maria Mulder, Dr. Moerland Anke and Dr. Dalindyebo Shabalala. Because of their friendship and help, I feel like be part of IGIR big family.

During my PhD, I was lucky enough to conduct my research for about 2 years at Max Planck Institute for Innovation and Competition. Hereby I would like to show my great gratitude to Prof. Reto Hilty, the director of the Institute. Because of his support, I got the opportunity to study in this distinguished Institute and learn German, which will benefit my academic career greatly in the future. Particularly, in the last year when my scholarship from CSC has ended, he granted me a contract with funding for 6 months, which help me through the toughest period of my PhD. Special thanks go to Prof. Matthias Leistner and Dr. Prof. Silke von Lewinski for their help in the German parts of my thesis. I also would like to thank my friends and colleagues at the Institute, and special thanks are due to Prof. Xuelong Peng, Prof. Lianfeng Wang, Dr. Mackenrodt Mark Oliver, Dr. Fischmann Filipe, Dr. Wei Zhuang, Lizhou Wei, Tao Li, Qiang Yu, Wentao Zhang and Ping Jiao. Their friendship and support help me a lot in the aspects of both research and living.

Feeling at home in Maastricht cannot be possible without the big Chinese community here. In a city that ten thousand miles away from our home, we become much closer than we could have ever reached in China. Special thanks go to Dr. Tianxiang He, Yaojin Peng, Tian Lv, who shared an office with me, and I cannot count how much insightful discussion we had in the office; Xiahong Chen, Jing Liu, who, as the forerunners coming to Maastricht, help me get used to the local life easier and faster; Wenqin Liao and Taotao Yue, who started their PhD at the Law Faculty in the same year as me; Jiangqiu Ge, Liuhu Luo, Liang Yu and many other Chinese colleagues who cheered up my life at Maastricht.

My family, particularly my parents, have been the pillar to support me to do this PhD project. Without their endless love and encouragement, I could not go through the hard time of my PhD, and finally finish it.
The last, but not least, I wish to thank my wife, Pei Zhang, for her great support during my PhD. We met, fell in love and got married in Maastricht. Thank Maastricht for bringing her into my life.

Introduction

Introduction

Today, ISPs[1] which host information directed at their subscribers, are commonly conducting business in an international market, some of them even successfully make their services part of netizens' daily life, such as YouTube, Facebook, and Twitter. In order to achieve commercial success on the international stage, it is necessary for hosting ISPs to know what legal risks they face, in other words their freedom to operate.

One of the legal risks originates from the dual use of hosting ISPs' services, and it is that their services can be used for both legal and illegal purposes. In particular, copyright owners always complain that their copyrighted materials are uploaded on hosting platforms without authorization.[2] Lawsuits have taken place between copyright owners and hosting ISPs worldwide. These lawsuits focus on dealing with whether hosting ISPs should be responsible for copyright infringement on their platforms and what kind of responsibilities should be imposed on them. Hence, in the context of copyright enforcement, the question of how much freedom to operate do hosting ISPs have is mainly dependent on the ambit of their responsibilities for copyright infringement.

Because copyright responsibility rules play a key role in regulating the freedom to operate of hosting ISPs, hosting ISPs may face the following two obstacles when conducting business on an international stage. First, hosting ISPs are obligated to undertake too many responsibilities against copyright infringement on their platforms, which unjustifiably shift the burden of enforcement from copyright owners to them. The unreasonable burden of enforcement may even stifle the freedom to operate of hosting ISPs. Second, in different jurisdictions hosting ISPs may be subject to different rules that regulate their responsibilities for copyright infringement, which exposes them to legal uncertainty when expanding their business in the international market.

This is the starting point of this research, which analyzes the importance of copyright responsibility rules in regulating the freedom to operate of hosting ISPs, and the legal obstacles faced by hosting ISPs when conducting business internationally. In order to remove these legal obstacles rooted in copyright responsibility rules, this research

1 ISP is the abbreviation of Internet service provider. According to the definition in the Digital Millennium Copyright Act (thereafter DMCA), an Internet service provider "means a provider of online services or network access, or the operator of facilities therefor." See DMCA Sec. 512 (k)(B). In the light of the definition in E-commerce Directive, an Internet service provider means " any natural or legal person providing an information society service". See Council E-commerce Directive of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L 178/1 (thereafter E-commerce Directive), Art. 2. Regarding "information society service," it means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. See Council Directive 98/48/EC of 20 July 1998 on amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, Art. 1(2). Therefore, ISP is a broad concept which covers a wide range of natural and legal persons who provide services on the Internet at the request of the recipients of their services.

2 For example, Viacom claimed that more than 150, 000 clips of its copyrighted materials were available on YouTube without authorization, and these clips had been viewed "an astounding 1.5 billion times," so it demanded 1 billion US dollars in damages. See *YouTube law fight 'threatens net'*, BBC(2008), *available at* http://news.bbc.co.uk/2/hi/technology/7420955.stm. See also *Viacom International, INC. v. YouTube, INC.*, 718 F. Supp. 2d 514 (S.D.N.Y. 2010), *Viacom International, INC. v. YouTube, INC.*, 676 F.3d 19 (2nd Cir. 2012).

discusses the copyright responsibilities imposed on hosting ISPs in different jurisdictions (US, EU and China), and then examines how the responsibilities rules affect the freedom to operate of hosting ISP in these jurisdictions. Eventually, based on this examination, this research proposes how to regulate hosting ISPs' copyright responsibilities from the perspective of preserving maximum freedom for them to operate. The aim of this book is therefore to contribute to establishing the freedom to operate of hosting ISPs through examining and tailoring the rules of their copyright responsibilities in the US, EU and China. By doing so, it is submitted that hosting ISPs' freedom to operate can be maximized in the context of online copyright enforcement so that they can face less legal uncertainty when conducting business internationally.

To introduce the specific research questions, this chapter first explores the background of preserving the freedom to operate of hosting ISPs in the context of copyright enforcement (1.1). After this exploration, it presents the definition of the problem (1.2), and explains the methodologies and the outline of the book (1.3).

1.1 Background

In the early days of hosting services, because of the limited available bandwidth, only text materials could be posted on hosting platforms, such as Usenet newsgroups. However, with the development of Internet technologies, larger sized documents, including images, music, software and even high-resolution movies, can now be posted on hosting ISPs' platforms, and this has aroused the concern of copyright owners. Regarding these uploaded contents, some are posted by Internet users without authorization, which may constitute copyright infringement. In such cases, the Internet users who post infringing materials should in principle be held liable. However, because of the anonymization on the Internet, it is in fact impossible for copyright owners to identify these Internet users who commit copyright infringement and then ask them to assume liability. Further, it is also much less cost-effective to target Internet users, since illegal use occurs in high volume while the return from suing Internet users is really low.[3] Therefore, copyright owners turn to hosting ISPs, who act as intermediaries and facilitators of distributing infringing materials, and claim that hosting ISPs should be responsible for infringement committed by their subscribers.

In the US, EU and China, lawsuits between copyright owners and hosting ISPs have been occurring on a large scale. In the US, a large number of hosting ISPs, including for example Netcom,[4] Veoh,[5] Rapidshare,[6] YouTube,[7] have been sued by copyright

3 Lemley MA. and Reese RA, 'Reducing digital copyright infringement without restricting innovation' (2004) 56 Stanford Law Review 1345 at 1349.

4 *Religious Technology Center v. Netcom On-line Communications Services*, 907 F. Supp. 1361 (N.D. Cal. 1995).

5 *Io Group, Inc v. Veoh Networks, Inc.*, 586 Supp.2d 1132 (C.D.Cal. 2008).

6 *Perfect 10, Inc. v. RapidShare*, No. 09-CV-2596 H (S.D. Cal., 2010).

7 *Viacom International, INC. v. YouTube, INC.*, 676 F.3d 19 (2nd Cir. 2012).

owners for the infringement on their platforms since the first of such cases occurred in 1993 where Frena was sued by Playboy as its copyrighted pictures were illegally posted on Frena's BBS[8]. In the EU, hosting ISPs, such as YouTube, Myspace, Dailymotion, Rapidshare, have also faced many lawsuits against them based on copyright infringement claims.[9] In China, hosting ISPs faced a vast number of lawsuits launched by copyright owners, and for example, in January and February of 2009 alone, the Beijing Haidian District Court received more than 70 indictments requesting video-sharing websites to be liable for videos illegally posted by the subscribers.[10] Such a large amount of lawsuits against hosting ISPs poses a big threat to their freedom to operate.

So far, the legislators in the US, EU and China have commonly adopted "safe harbor" provisions that exempt hosting ISPs from monetary liability under certain conditions,[11] which can help to ensure the freedom to operate of hosting ISPs. This section gives an overview of preserving the freedom to operate of hosting ISPs in the context of online copyright enforcement. It first looks back to "safe harbor" provisions, and explores the reasons to grant hosting ISPs liability privileges so as to ensure their freedom to operate (Section 1.1.1). Then, it explores the factors that justify the restriction of hosting ISPs' freedom to operate in the light of "safe harbor" provisions (Section 1.1.2). Finally, it presents an overview of the rules that regulate hosting ISPs' responsibilities for copyright infringement, and then addresses the challenges they bring to hosting ISPs in operation (Section 1.1.3).

16

1.1.1 Liability Privileges to Ensure the Freedom to Operate of Hosting ISPs

On the Internet, as copyright infringement is running rampant, for the sake of protecting copyright, ISPs, as gatekeepers on the Internet, may be ideally placed to take charge of copyright enforcement.[12] However, "safe harbor" provisions still grant ISPs liability privileges, which helps to ensuring the freedom to operate. ISPs' freedom to operate can be justified, because it contributes to promoting several social interests, which will be explored below.

8 *Playboy Enterprises Inc. v. Frena*, 839 F.Supp. 1552 (M.D. Fla. 1993). BBS is the abbreviation for a bulletin board system. It is a computer server running custom software that allows users to connect to the system using a terminal program. Once logged in, the user can perform functions such as uploading and downloading software and data, reading news and bulletins, and exchanging messages with other users through email, public message boards, and sometimes via direct chatting. See Bulletin board system, Wikipedia, *available at* https://en.wikipedia.org/wiki/Bulletin_board_system (last visited 09-02-2014).

9 These cases will be discussed in Chapter 3 and Chapter 4.

10 Wang HC (王宏丞) and Cao LP (曹丽萍) and Li DT (李东涛), 'Study on the Key Points in the Cases of Infringement on Video-sharing Websites (论视频分享网站侵权案件中的焦点问题)' (2009) 4 Electronic Intellectual Property (电子知识产权) 11 at 12.

11 See DMCA (n1), Sec. 512; E-commerce Directive (n1), Section 4; Internet Regulation (信息条例) (n1), Art. 14-17, Art. 20-25.

12 See Ginsburg JC, 'Putting Cars on the" Information Superhighway": Authors, Exploiters, and Copyright in Cyberspace' (1995) 95 Columbia Law Review 1466; Lichtman D and Landes W, 'Indirect liability for copyright infringement: an economic perspective' (2003) 16 Harvard Journal of Law & Technology 395; Carmichael J, 'In Support of the White Paper: Why Online Service Providers Should Not Receive Immunity from Traditional Notions of Vicarious and Contributory Liability for Copyright Infringement' (1995) 16 Loyola of Los Angeles Entertainment Law Review 759.

The first justification is for promoting e-commerce. The importance of promoting e-commerce has been widely recognized in the documents relevant to "safe harbor" provisions. For example, the E-commerce Directive clearly states that "the development of electronic commerce within the information society offers significant employment opportunities in the Community, particularly in small and medium-sized enterprises, and will stimulate economic growth and investment in innovation by European companies, and can also enhance the competitiveness of European industry…"[13] Even before the E-commerce Directive was enacted, there were already several reports published by the EU Commission which announced the importance of developing e-commerce. According to these reports, in order to facilitate e-commerce, it is necessary to clarify the responsibility of ISPs who transmit and store the information from third parties.[14] In fact, "safe harbor" provisions, which grant ISPs liability privileges, do help to fulfil the policy aim of promoting e-commerce. According to the EU Commission, "safe harbor" provisions raise the legal certainty for Internet intermediaries, which reduces their business risks and expenses for legal consultants, and encourages the start-up in the Internet intermediary industry.[15] Further, in the US, a House Report which was drafted by the Commerce Committee before enacting DMCA named e-commerce as the emerging digital economy.[16] At the end of 1997, about 7.4 million Americans were employed in the sectors relevant to e-commerce.[17] In addition, this report also expected that e-commerce would grow very quickly, and that by 2002 the value of e-commerce would "range from $200 billion to more than $500 billion, compared to just $2.6 billion in 1996."[18] Since the growth of e-commerce has had a profound influence on a nation's economy and job market, promoting e-commerce should be taken into account when drafting the DMCA.[19] In China, to promote the development of the Internet industry which is an important part of e-commerce, the Internet Regulation grants ISPs liability exemptions on certain conditions by referring to the DMCA and the E-commerce Directive.[20]

The second justification is to ensure the efficiency of the Internet. In order to maintain the efficiency of the Internet, Internet intermediaries including hosting ISPs can only process such a large amount of information automatically. The Internet is characterized by efficiency in transmitting information, and information can be distributed on vast

13 E-commerce Directive (n1), Recital 2.

14 See IP/97/313, Electronic Commerce: Commission Presents Framework for Future Action, 16 April 1997. IP/98/999, Electronic Commerce: Commission Proposes Legal Framework, 18 November 1998.

15 Nielson CK, Jervelund C, Pedersen KG, Rytz B, Hansen ES, Ramskov JL, 'Study on The Economic Impact of the Electronic Commerce Directive' (2007), European Commission, DG InternalMarket and Services Unit E2, at 17.

16 Congress, U. S., House Report 105-551 (1998), Part II (thereafter H.R. REP. 105-551(II)), at 21.

17 Ibid.

18 Ibid

19 Ibid, at 22.

20 Zhang JH (张建华), *The Interpretation of Regulation on the Protection of the Right to Internet Dissemination of Information (信息网络传播权保护条例释义)* (China Legal Publishing House (中国法制出版社) 2006), at 85.

scales at unprecedented speeds on the Internet. Internet intermediaries substantially contribute to the aforesaid efficiency, since they process hundreds of millions of data transmissions each day, and host or link to tens of billions of items of third party content.[21] Taking YouTube as an example, in 2015, more than 100 hours of videos were uploaded to it every minute.[22] In this regard, hosting ISPs are different from traditional publishers, because the latter need to choose, edit or even censor the content from third parties before distributing it. If hosting ISPs were required to undertake strict liability for copyright infringement as publishers do, they then would be forced to monitor the content uploaded by Internet users, which would unavoidably reduce the efficiency of internet transmission. Further, because the Internet today has become an important way for the public to access information and knowledge,[23] then if Internet transmission becomes less efficient, it will decrease the public's ability to access information and knowledge. A report conducted by the United Nations Human Rights Council has even argued that, if holding ISPs liable for the content transmitted or created by Internet users, freedom of speech would be seriously undermined, in the words of UN Human Rights Council: "it leads to self-protective and over-broad private censorship, often without transparency and due process of law."[24]

The third justification is to foster the development of Internet technologies. As noted by Jennifer Bretan, if no measure is adopted to protect ISPs from crushing liability, ISPs cannot provide the technical backbone to support the Internet anymore.[25] Therefore, ISPs, as the entities who develop and implement Internet technologies, ought to be granted liability privilege so as to guarantee their freedom to operate, and otherwise they would lack the motivation to develop and apply new Internet technologies.[26] This argument reflects the wisdom of liability rules that deal with the tension between copyright protection and dual-use technologies in the offline

21 Lemley MA, 'Rationalizing Internet Safe Harbors' (2007) 6 Journal of Telecommunications and High Technology Law 101, at 101.

22 Statistics, YouTube(2015), *available at* http://www.youtube.com/yt/press/statistics.html (last visited 21-09-2015).

23 As noted by the European Court of Human Right, "In the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the sharing and dissemination of information generally." See Application nos. 3002/03 and 23676/03 Times Newspapers Ltd (nos. 1 and 2) v. the United Kingdom [2009] EMLR 14, ECHR.

24 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations General Assembly, A/66/290, 10 August 2011, at 12.

25 Bretan J, 'Harboring Doubts about the Efficacy of 512 Immunity under the DMCA' (2003) 18 Berkeley Technology Law Journal 43, at 43.

26 See generally Lemley and Reese, 'Reducing digital copyright infringement without restricting innovation' (n3), at 1386-1390. In this article, the authors demonstrate that if holding facilitators liable for the copyright infringement committed by their users, facilitators would not develop or apply new technologies to improve their services or products, which would obviously restrict the technological innovation.

world.[27] As noted by Ginsburg, in order to keep the copyright incentive meaningful, it is necessary to grant copyright owners sufficient control over new ways of using their works, but not so much as to "stifle the spread of the new technologies of dissemination."[28] In addition, promoting the development of technologies may generate the so-called "spillover" effects believed by Mark Lemley.[29] He argues that "economic evidence strongly suggests that those unanticipated future benefits, or 'spillover' effects, often exceed the immediate value of most new technologies."[30] The video tape recorder technology discussed in the Sony case is a good example. After the Sony case, copyright owners later found video tape recorders could bring them a new and enormously profitable channel of distributing their works, and in the late 1990s, more than six millions units of video cassettes were rented or sold each year.[31] Today, the "spillover" effects of hosting technologies have already started to benefit copyright owners, because hosting ISPs and copyright owners have reached many agreements which allow copyright owners to share the revenue of hosting ISPs.[32]

27 In the early 1980s, Sony started to sell video tape recorders which could be used to record television programs, and finally, the US Supreme Court held that since the video tape recorders sold by Sony were capable of substantial non-infringing uses, the company was not liable for selling a product that might be used for infringing purposes. See Sony Corp. of America v. Universal City Studios, 464 U.S. 417 (1984). In the UK, Amstrad Consumer Electronics sold blank tapes with twin cassette decks which enabled the high speed copying of a recording from one tape to another, and eventually, the House of Lords rejected Amstrad's copyright liability, because the blank tapes enabled the recording and copying of copyrighted materials, but such recording and copying might or might not be unlawful. C.B.S. Songs Ltd and ors v. Amstrad Consumer Electronics Plc [1988] 1 A.C. 1013. If the defendants in these two cases were held liable for copyright infringement, the technologies concerned would be banned.

28 Jane C Ginsburg, *Copyright and control over new technologies of dissemination*, Columbia Law Review (2001). 1613-1614.

29 Lemley and Reese, 'Reducing digital copyright infringement without restricting innovation' (n3), at 1387.

30 Ibid.

31 Liu JR, 'Why is Betamax an Anachronism in the Digital Age?–Erosion of the Sony Doctrine and Indirect Copyright Liability of Internet Technologies' (2005) 7 Vanderbilt Journal of Entertainment and Technology Law 243, at 353.

32 For instance, since 2006, YouTube has signed a series of agreements with several copyright giants, including Warner Music Group, CBS Corporation, Universal Music Group and Sony BMG. According to these agreements, copyright owners can share the advertising revenue collected not only from videos in their brand channels, but also from the user-generated videos that incorporate the audio and audiovisual works copyrighted by them on YouTube. See Warner Music Group and YouTube Announce Landmark Video Distribution and Revenue Partnership, Warner Music Group(2006), *available at* http://investors.wmg.com/phoenix.zhtml?c=182480&p=irol-newsArticle&ID=906153 (last visited 09-02-2013); CBS and Youtube Strike Strategic Content And Advertising Partnership, CBS Corporation (2006), *available at* http://www.cbscorporation.com/news-article.php?id=23 (last visited 09-02-2013); Universal Music Group and YouTube Forge Strategic Partnership, Universal Music Group(2006), *available at* http://www.universalmusic.com/corporate/detail/393 (lasted visited 13-09-2013); Sony BMG Music Entertainment Sighs Content License Agreement with YouTube, Sony Music(2006), *available at* http://www.sonymusic.com/sonymusic/sony-bmg-music-entertainment-signs-content-license-agreement-with-youtube/ (lasted visited 13-09-2013). In the EU, Dailymotion have also signed similar agreements with wide range of copyright owners, and in the light of these agreements, copyright owners can get as much as 70% of all advertising revenue created by their contents. See http://official.dailymotion.com/en/ (lasted visited 15-09-2013). In China, Youku has signed corporation agreements with Sony Pictures Entertainment, Warner Brother, Dreamworks, Paramount, 21st Century Fox, Disney, and other copyright owners. See YoukuTudou signed a 5-year copyright licensing contract with Sony Picture (优酷土豆与索尼音像签订五年版权协议), it.sohu.com(2012), *available at* http://it.sohu.com/20121106/n356832451.shtml (lasted visited 18-09-2013).

1.1.2 Justification of Imposing Restriction on the Freedom to Operate of Hosting ISPs

Section 1.1.1 demonstrates that ensuring the freedom to operate of hosting ISPs can benefit several social interests. Therefore, it is reasonable for "safe harbor" provisions to grant hosting ISPs liability privilege so as to ensure their freedom to operate. Nevertheless, the liability privilege granted to hosting ISPs is not absolute. In fact, "safe harbor" provisions also indicate that restrictions may be imposed on the freedom to operate of hosting ISPs for the purpose of protecting other's interests. In the EU, the liability rules of intermediaries should strike a delicate balance between the different interests concerned and promote cooperation between different parties so as to reduce the infringement on the Internet.[33] The legislative document of DMCA also notes that it is necessary to balance the interests of copyright owners, online service providers and information users in a proper way so as to foster the development of e-commerce.[34] In China, Internet Regulation also aims at reconciling the interests of copyright owners, ISPs and Internet users.[35] Therefore, copyright protection and Internet users' interests may justify imposing restriction on hosting ISPs' freedom to operate in the US, EU and China.

Without imposing copyright responsibilities on hosting ISPs, hosting platforms would be recklessly used for copyright infringement, and hosting ISPs may even promote
20 the infringing use of their services for profit. Therefore, it is commonly accepted that restriction ought to be imposed on hosting ISPs' freedom to operate for the purpose of protecting copyright. In light of "safe harbor" provisions, hosting ISPs can be exempted from copyright liability only when they comply with prescribed conditions.[36] Further, "safe harbor" provisions merely exempt a hosting ISP who complies with prescribed conditions from paying monetary damages, but regarding the other kind of reliefs, such as injunction, "safe harbor" provisions do not immunize hosting ISPs from them.[37] Therefore, even though "safe harbor" provisions have been adopted in the US, EU and China, hosting ISPs are still subject to several obligations of reinforcing copyright protection on their platforms.

33 IP/98/999 'Electronic Commerce: Commission Proposes Legal Framework' (n14).

34 H.R. REP. 105-551(II) (n16),, at 21.

35 *Legislative Affair Office Answered Reporters' Questions on "Regulation on the Protection of the Right to Internet Dissemination of Information" (法制办就《信息网络传播权保护条例》答记者问)*, xinhuanet.com (新华网) (2006), *available at* http://news.xinhuanet.com/politics/2006-05/29/content_4615669.htm.

36 For instance, hosting ISPs need to comply with several requirement so as to be exempted from monetary liability. Further, hosting ISPs also need to fulfill certain obligations in notice-and-takedown procedures and identity disclosure mechanisms according to "safe harbor" provisions. See generally DMCA § 512, Internet Regulation, E-commerce Directive Section 4. These duties will be discussed in detail in the following chapters.

37 See DMCA (n1), Sec. 512, (c)(1); E-commerce Directive (n1), Art. 14; Internet Regulation (网络条例) (n1), Art. 22.

Internet users' interests also affect how to define hosting ISPs' freedom to operate. As has been demonstrated in Section 1.1.1, ensuring the freedom to operate of hosting ISPs contributes to promoting e-commerce, keeping the efficiency of the Internet and fostering the development of Internet technologies. These three benefits cater for Internet users' interests, so in this sense, Internet users' interests help to justify ensuring the freedom to operate of hosting ISPs. In addition, Internet users' interests are concerned in tailoring hosting ISPs' obligations for copyright protection, because when hosting ISPs fulfill these obligations, it may raise the concerns on Internet users' human rights, including freedom of speech and privacy.[38]

For example, notice-and-takedown procedures have been widely adopted so as to efficiently remove infringing materials from hosting platforms.[39] Nevertheless, this procedure not only facilitates the takedown of infringing materials but also results in the deletion of lawful materials, which may freeze freedom of expression.[40] Further, in order to ensure the copyright owners' right to sue anonymous Internet users, ISPs are required to disclose the Internet users' identities under certain circumstances, which can be named as "identity disclosure mechanism".[41]

38 See Seltzer W, 'Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment' (2010) 24 Harvard Journal of Law & Technology 171. Rantou MI, The growing tension between copyright and personal data protection on an online environment: The position of Internet Service Providers according to the European Court of Justice (2012) 3 European Journal of Law and Technology 2.

39 In the US and China, the notice-and-takedown procedure has been adopted into the "safe harbor" provisions, see DMCA (n1) 512 (c), (f), (g), and Internet Regulation (信息条例) (n1), Art. 14-17. In the EU, although E-commerce Directive has not adopted notice-and-takedown procedure, in the member states the statutory or self-regulatory notice-and-takedown procedures have been widely adopted. See Commission Staff Working Paper: Online Services, Including E-commerce, in the Single Market, SEC (2011) 1641 final, 11 January 2012, at 39-46.

40 In order to protest against the misuse of takedown notices, a website called "Chilling Effects Clearinghouse" has been set up to allow the public to report the notices they receive. See https://www.chillingeffects.org/index.cgi, (last visited 22-08-2014). In the light of research done on the 876 notices reported to Chilling Effects, Urban and Quilter noted that nearly 30% of takedown notices sent to Google were based on flawed or highly questionable copyright claims. See Urban JM and Quilter L, 'Efficient Process or Chilling Effects-Takedown Notices under Section 512 of the Digital Millennium Copyright Act' (2005) 22 Santa Clara High Technology Law Journal 621, at 667. Another research done by the Brennan Center for Justice at New York University revealed that, among 245 takedown notices reported to Chilling effects in 2004, 63% of the notices "either targeted material with a fair use/First Amendment defense or stated a weak IP claim." See Heins M and Beckles T, *Will Fair Use Survive? Free Expression in the Age of Copyright Control* (Brennan Center For Justice 2005), at 35.

41 In the US, DMCA 512 (h) grants copyright owners the rights to apply subpoenas for the purpose of disclosing Internet users' identities. In China, according to Article 13 of Internet Regulations, the administrative department of copyrights may, with the purpose of investigating the infringements upon the right to network dissemination of information, require the relevant Internet service provider to provide such materials as the names, contact information, and the web address of its service objects who are suspected of committing copyright infringement. Further, in terms of Internet Interpretation (2006), copyright owners also can request the registration information of Internet users from hosting ISPs for the purpose of suing the Internet users for copyright infringement. In the EU, there are several directives indicating that Internet users' data can be disclosed for the purpose of protecting copyright, see Article 13 of General Data Protection Directive (Directive 95/46/EC), Article 15 of E-privacy Directive (Directive 2002/58/EC), Article 15(2) of E-commerce Directive and Article 8 of IP Enforcement Directive (Directive 2004/48/EC).

Yet, the disclosure of Internet users' identities may conflict with their privacy.[42] In addition, anonymity is considered to play an important role in guaranteeing freedom of expression, because anonymity not only allows the public to deliver freely their opinions about "their interests, beliefs and political ideologies without fear of reprisals from the state or any other powerful organization," but also "permits others to receive these views."[43] Therefore, the obligation of disclosing Internet users' identities may also conflict with freedom of speech. Besides, filtering technologies have been widely adopted by hosting ISPs so as to reduce copyright infringement on their platforms,[44] which raises the concerns about accommodating fair use.[45] Therefore, filtering technologies may result in over-filtering, which negatively affects the freedom of speech enjoyed by Internet users.

1.1.3 Operating Challenges for Hosting ISPs in the US, EU and China

For a hosting ISP which is operating or planning to operate in the US, EU and China, it may face two challenges resulting from the copyright responsibility rules in these three jurisdictions. First, copyright responsibilities imposed on hosting ISPs are diverse in the US, EU and China, and this poses legal uncertainty in front of hosting ISPs. Second, responsibility rules impose unreasonable burdens on hosting ISPs in some cases.

Hosting ISPs, as facilitators of information transmission on the Internet, may assume
22 secondary liability for the infringing materials posted by their subscribers. As will be seen in Chapter 2, rules of indirect copyright infringement in the US, EU and China are diverse. In the US, contributory infringement and vicarious liability have been

42 Cohen JE, 'Overcoming Property: Does Copyright Trump Privacy?' (2002) 2002 Journal of Law, Technology & Policy 375, at 375. Katyal S, 'Privacy vs. Piracy' (2004) 7 Yale Journal of Law & Technology 222, at 335-345. Edwards L, 'Should ISPs be Compelled to Become Copyright Cops? File-Sharing, the Music Industry and Enforcement Online' (2009) 19 Journal of the Society for Computers and Law 29. In these articles, the authors argue that copyright protection endangers privacy.

43 Williams KS, 'On-Line anonymity, deindividuation and freedom of expression and privacy' (2005) 110 Penn State Law Review 687, at 687.

44 Case law in some jurisdictions requires hosting ISPs to adopt reasonable filtering technologies, see BGH 15 August 2013, No. I ZR 80/12, *Han Han v. Baidu (韩寒诉百度)*, Beijing Haidian District Court, No. 5558 Hai Min Chu Zi (2012) (2012海民初字第5558号). Further, in light of self-regulation agreements, hosting ISPs also need to adopt filtering technologies, see Principles for User Generated Content Services (2007), *available at* http://www.ugcprinciples.com/ (last visited 12-06-2015); self-discipline treaty on Internet audio-video program services in China (中国互联网视听节目服务自律公约), State Administration of Radio Film and Television (国家广电总局)(2008), *available at* http://www.sarft.gov.cn/articles/2008/02/22/20080226114116260491.html (last visited 16-06-2015). YouTube also establishes its own filtering system named "Content ID", see How Content ID works, *available at* https://support.google.com/youtube/answer/2797370?hl=en (last visited 18-06-2015).

45 Sawyer MS, 'Filters, Fair Use & Feedback: User-Generated Content Principles and the DMCA' (2009) 24 Berkeley Technology Law Journal 363, at 366. In this article, Sawyer asserts that given that fair use is such a major challenge for the courts to evaluate, it is almost impossible for any technological solution to reach accurate determinations. See also Fair Use Principles for User Generated Video Content, Electronic Frontier Foundation (2007), *available at* https://www.eff.org/pages/fair-use-principles-user-generated-video-content (last visited 28-07-2014). In this report, Electronic Frontier Foundation (EFF) also claims that filtering technologies can hardly accommodate fair use.

developed by case law;[46] in the EU, different Member States rely on different rules to regulate indirect copyright infringement;[47] in China, courts refers to joint infringement theory when deciding the cases about indirect copyright infringement, and particularly assess whether a defendant fulfills his duty of care to prevent infringement.

Liability privileges rules in the US, EU and China have reached a certain degree of harmonization, but differences still exist in many aspects.[48] First, "Safe harbor" provisions have been adopted in the US, EU and China, and they share many common points. For instance, hosting ISPs have no general obligation to monitor the materials uploaded on their platforms.[49] Further, in order to benefit from liability exemption, hosting ISPs should not know the infringement in question, or upon knowing the infringement, they should expeditiously remove the infringing materials.[50] Third, hosting ISPs are obligated to disclose suspected users' identities to copyright owners or competent authorities under prescribed conditions.[51] Nevertheless, "safe harbor" provisions in the US, EU and China still include several different provisions. For example, the US and China have codified notice-and-takedown procedures in their "safe harbor" provisions, but the E-commerce Directive leaves this procedure for the Member state to develop by themselves.[52] Further, the "safe harbor" provisions in the US include a provision which requires hosting ISPs to terminate the accounts of subscribers who commit infringements repeatedly,[53] but the EU and China have not adopted this provision in their "safe harbor" provisions. Besides, as will be seen in Chapter 2, there are still several other differences existing between "safe harbor" provisions in the US, EU and China. Furthermore, as will be demonstrated in Chapter 3, 4, 5 and 6, even regarding those same or similar provisions, courts in different jurisdictions tend to interpret them in different ways, which results in different impacts on hosting ISPs' freedom to operate.

Some responsibility rules developed by case law may impose an unreasonable burden on hosting ISPs. As will be seen in Chapter 4, in order to better protect copyright on hosting platforms, a certain effort has been made to reinforce hosting ISPs' responsibilities for copyright infringement. Regarding secondary liability, the courts in the US, EU and

46 Regarding what are contributory infringement and vicarious liability, see Sec. 2.1.1.

47 As presented in Chapter 2, the UK has developed authorization infringement and joint tortfeasance, but the civil law countries, such as Germany, France and Italy, the courts usually decide the indirect copyright infringement cases by referring to the general liability rules, particularly the duty of care notion, in tort law.

48 As noted by Daniel Seng, "safe harbor" provisions have indeed become a global standard to limit ISPs' liability for indirect copyright infringement, but interpretational problems still exist. See Seng D, Comparative Analysis of National Approaches of the Liability of the Internet Intermediaries (Preliminary Version), para. 6, *available at* http://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries.pdf (last visited 04-03-2016).

49 DMCA (n1), Sec. 512, (m) (1); E-commerce Directive (n1), Art. 15.

50 DMCA (n1), Sec. 512 (c) (1) (A); E-commerce Directive (n1), Art. 14, 1; Internet Regulation (网络条例) (n1), Art. 22 (3).

51 DMCA (n1), Sec. 512 (h); E-commerce Directive (n1), Art. 15; Internet Regulation (网络条例) (n1), Art. 15-17, Art. 24.

52 DMCA (n1), Sec. 512 c (3) and g; E-commerce Directive (n1), Recital 40.

53 DMCA (n1), Sec. 512 (i).

China tend to decide hosting ISPs' liability by taking into account some factors which are not prescribed in "safe harbor" provisions, such as the hosting ISPs' intent and business model, specific monitoring obligations against repeat infringement, and better protection for highly valuable contents.[54] Strong arguments can be found to support the courts to take into account these factors. However, in the light of case law in these jurisdictions, these factors, including imputed intent, illegal business model and specific monitoring obligation, can easily be too broadly interpreted by courts, which may stifle hosting ISPs' freedom to conduct legal business.[55] Further, as will be seen in Chapter 5, if the following questions are not properly dealt with, notice-and-takedown procedures would also impose an unreasonable burden on hosting ISPs. These questions are: how to define a competent notice, how to deal with defect notices, how to define "expeditiously removing", how to regulate the liability of wrong removing, and whether the validity of ex ante notices should be recognized.[56]

1.2 Definition of the Problem

"Safe harbor" provisions have been commonly adopted in the US, EU and China so as to ensure the freedom to operate of hosting ISPs. Some strong arguments, including promoting e-commerce, keeping the efficiency of the Internet and fostering the development of information technologies, can be built to justify granting liability privileges to hosting ISPs. Nevertheless, the liability privileges granted to hosting ISPs are conditional rather than absolute, because as revealed by the legislative documents relevant to "safe harbor" provisions, the freedom to operate of hosting ISPs can be restricted for the sake of protecting copyright and Internet users' interests.

In the US, EU and China, the rules of indirect copyright infringement are diverse. Further, although a certain level of harmonization has been reached in respect of liability privilege rules, these rules still include some different provisions, and more importantly, even regarding these similar or same provisions, the courts in the US, EU and China tend to interpret them in different ways. Therefore, hosting ISPs are exposed to diverse copyright responsibilities in the US, EU and China, which poses legal uncertainty for them when conducting business in these jurisdictions. In addition, the courts in the US, EU and China may interpret copyright responsibility rules in ways that impose too much burden on hosting ISPs, which unreasonably restricts their freedom to operate.

This book aims at answering a main research question: *how to regulate hosting ISPs' responsibilities for copyright infringement while preserving their maximum freedom to operate in the US, EU and China?*

So far, hosting ISPs' copyright responsibilities, which affect how much freedom to

54 See Section 4.7.
55 Ibid.
56 See Section 5.4.

operate can be preserved to hosting ISPs, have mainly come from three sources, and they are copyright liability, facilitating obligations and self-regulatory duties. Regarding copyright liability, hosting ISPs do not upload infringing content by themselves, but as intermediaries, they may need to undertake secondary liability for the copyright infringement committed by their users. Nevertheless, in order to ensure hosting ISPs' freedom to operate, "safe harbor" provisions grant hosting ISPs liability exemptions under prescribed conditions. Besides secondary liability, hosting ISPs also need to fulfill certain obligations, such as taking down infringing materials upon receiving competent notices and disclosing Internet users' identities to copyright owners, so as to facilitate copyright enforcement on their platforms. These two levels of responsibilities are regulated by the state regulation, including legislation, case law and administrative orders. The third level of responsibility means the duties that need to be fulfilled by hosting ISPs in terms of self-regulatory norms mainly reached between private entities. Self-regulation prevails, since the traditional regulatory norms fail to settle the disputes between copyright owners and hosting ISPs.[57]

Based on the above observation, to answer the main research question, this book focuses on addressing the following sub-questions:

(i) *Should hosting ISPs be required to keep purely passive so as to fall under "safe harbor" provisions;*
(ii) *How do the courts interpret the factors that are relevant to decide hosting ISPs' copyright liability under "safe harbor" provisions; and*
(iii) *Whether the liability criteria that are developed by the case law are capable of preserving maximum freedom for hosting ISPs to operate;*
(iv) *How notice-and-takedown procedures ought to be interpreted so as to avoid imposing unreasonable duties on hosting ISPs; and*
(v) *Whether hosting ISPs should be given more duties to ensure the accuracy of notices;*
(vi) *How hosting ISPs' duties ought to be tailored in identity disclosure mechanisms;*
(vii) *Whether self-regulation can better preserve the freedom to operate of hosting ISPs.*

This book discusses how to preserve maximum freedom to operate for hosting ISPs in the context of online copyright enforcement, so it will only deal with how copyright responsibility rules may restrict hosting ISPs' freedom to operate in the US, EU and China. As for other rules which may impose restrictions on hosting ISPs' freedom to operate, this book will not take them into account. Hence, this book will not assess how the censorship regime in China restricts hosting ISPs' freedom to operate. Further, in operation, hosting ISPs collect Internet users' personal data and exploit these data commercially, which may commit privacy violation. The restrictions resulting from

57 Hugenholtz PB, 'Codes of Conduct and Copyright Enforcement in Cyberspace' *in* Stamatoudi IA (eds), *Copyright Enforcement and the Internet* (Kluwer Law International, 2010), at 303.

privacy laws in this context will not be discussed in this book, and it will only evaluate how privacy protection affects the copyright responsibilities imposed on hosting ISPs, particularly in identity disclosure mechanisms. In addition, for hosting ISPs which acquire a position of dominance in the market may also face anti-trust violation complaints, and this book will not discuss restrictions based on anti-trust concerns. Moreover, although this study covers several jurisdictions, it will not discuss the issue of whether and how the copyright responsibility rules in one jurisdiction can be applied in another jurisdiction, so private international law is outside of the scope of this study. Finally, the EU and the US have been active in negotiating multilateral and bilateral trade agreements which may also include some clauses that regulate hosting ISPs' responsibilities for copyright infringement, such as Anti-Counterfeiting Trade Agreement (ACTA). However, lots of concerns on protecting fundamental rights has been raised against these trade agreements, and ACTA was even rejected by the European Parliament in 2012.[58] Therefore, it is still unclear how these trade agreement affect hosting ISPs' copyright responsibilities, and this book will not discuss about them.

1.3 Methodology and Outline of the Book

To answer the research questions stated above, this book mainly takes a comparative
26 approach to examine how hosting ISPs' responsibilities for copyright infringement is dealt with in the US, EU and China. Because the Internet is borderless, hosting ISPs conceptually conduct business in an international market. In fact, many hosting ISPs are conducting business or at least are willing to conduct business internationally. The US, EU and China are the 3 largest economies in the world, so ambitious hosting ISPs would naturally like to conduct business in these three markets. The comparison of copyright responsibilities imposed on hosting ISPs in these three jurisdictions will help hosting ISPs to assess the legal risks they face, and then draw a map of freedom to conduct business in these respective areas. Further, when dealing with hosting ISPs' responsibilities for copyright infringement, courts in the US, EU and China apply different rules or interpret substantially similar rules in different ways, which results in various impacts on hosting ISPs' freedom to operate. The comparison therefore also helps to find the best way of regulating hosting ISPs' copyright responsibilities in regard to preserving for them the maximum freedom to operate. Finally, "safe harbor" provisions play a vital role in regulating hosting ISPs' copyright responsibilities, since such provisions are not only related to deciding hosting ISPs' liability, but also relevant to the application of notice-and-takedown procedures and identity disclosure

58 Baraliuc I, Depreeuw S, and Gutwirth S, 'Copyright enforcement in the digital age: a post-ACTA view on the balancing of fundamental rights' (2013) 21 International Journal of Law and Information Technology 92, at 92-104.

mechanisms.[59] After the first "safe harbor" provisions were adopted in the US, the EU and China also enacted their own "safe harbor" provisions by referring to the US version. In this respect, a certain degree of harmonization has already been reached in regulating hosting ISPs' copyright responsibilities, and the author believes that further harmonization in interpreting "safe harbor" provisions will enhance hosting ISPs' freedom to operate in these jurisdictions. The comparison can help to evaluate whether and how the further harmonization can be done in the US, EU and China. To answer the last sub-question, the comparative study is still employed, because comparison needs to be done between state-regulatory norms and self-regulatory norms.

In the EU, since relevant Directives and ECJ decisions leave much room for member states to interpret related rules, in order to look deeper into how hosting ISPs' copyright responsibilities are regulated in the EU, this book also explores the legislations and case law in several member states. In fact, several member states have developed their own liability rules when applying "safe harbor" provisions, such as notice-and-staydown mechanism in France, disturber's liability in Germany, active hosting theory in Italy, authorization infringement and joint tortfeasor in the UK. These specific liability rules affect how much freedom a hosting ISP is allowed to operate, so in order to answer better the first three sub-questions, this book evaluates how hosting ISPs' copyright liability is regulated in these four member states under the auspices of the EU jurisdiction.

Further, regarding case study, since the EU "safe harbor" provisions not only cover online copyright disputes but also online trademark infringement, when discussing how the "safe harbor" provisions are interpreted by the courts in the EU, the related trademark cases are also analyzed, particularly these trademark cases decided by the ECJ and supreme courts in member states. In China, the hosting ISPs share the common notice-and-takedown procedure with the ISPs who run information location tools, so the case law of the latter is also under examination, when discussing how the Chinese courts interpret the notice-and-takedown procedure.

Besides the Introduction, this book consists of 7 chapters. Chapter 2 describes the rules of hosting ISPs' responsibilities for copyright infringement, including the liability rules about indirect copyright infringement and "safe harbor" provisions in the US, EU and China, which establish the basis for the analysis of relevant case law in the next four chapters. Although "safe harbor" provisions grant certain liability privileges to hosting ISPs, hosting ISPs should keep passive as a pre-condition to falling under "safe harbor" Provisions.

59 "Safe harbor" provisions not only include the rules on deciding whether hosting ISPs are monetarily liable for the infringement committed by their users, but also prescribe notice-and-takedown procedures and the disclosure of personal identity. See generally DMCA § 512, Internet Regulation, E-commerce Directive Section 4. Although E-commerce Directive does not include the detailed rules about notice-and-takedown procedures, because in light of Article 14, hosting ISPs need to immediately remove infringing materials upon knowing them, a de facto notice-and-takedown procedure has been widely recognized in the EU. Further, the Recital 14 of E-commerce Directive also refers to the Directives on privacy protection, and these Directives allow Internet users' identities to be disclosed for the purpose of copyright protection. The detailed discussion will be done in Chapter 2.

Chapter 3 takes a comparative approach to examine the relevant case law in the US, EU and China, and then summarizes on what basis the courts in these three jurisdictions hold hosting ISPs as not qualifying for keeping passive. Based on the comparison, this chapter suggests, in order to maximize hosting ISPs' freedom to operate, what factors should be taken into account by courts when deciding whether a hosting ISP keeps passive or not. After discussing the threshold of "safe harbor" provisions, Chapter 4 takes a comparative approach to analyze how the courts in the US, EU and China decide a hosting ISPs' liability under the roof of "safe harbor" provisions. This chapter summarizes the factors relevant to conclude liability, including general monitoring obligation, knowledge of infringement, receiving benefits, measures against repeat infringement and inducement, and then compare how the courts in each jurisdiction evaluate these factors. Finally, based on the comparison, this chapter identifies the tendencies regarding regulating the secondary liability of hosting ISPs from the perspective of case law. Then, it evaluates these liability rules developed from case law so as to check whether they are capable of preserving the maximum freedom to operate for hosting ISPs, and if not, how they should be adjusted.

Besides undertaking secondary liability under certain circumstances, hosting ISPs are also required to fulfill certain duties that facilitate copyright protection. In order to deal with the overwhelming copyright infringement on the Internet, the "safe harbor" provisions in the US and China codify notice-and-takedown procedures, according to which a hosting ISP should remove the alleged infringing materials after receiving competent notices. In the EU, although the E-commerce Directive does not include a detailed notice-and-takedown procedure, the notice-and-takedown procedures have been developed in member states, since after a hosting ISP receives the notices which can lead to its knowledge of infringing material, it is obligated to expeditiously remove the infringing materials. Chapter 5 compares the notice-and-takedown procedures in the US, EU and China, and analyzes how the courts in these jurisdictions interpret the key issues in notice-and-takedown procedures,[60] such as how to define a competent notice, how to deal with defective notices, how to define "expeditiously remove", how to regulate the liability of wrong deletion, and the validity of ex ante notices. Based on comparison, it concludes how these key issues ought to be interpreted so as to maximize hosting ISPs' freedom to operate. Besides, this chapter rethinks the current notice-and-takedown procedures in the US, EU and China, and then discusses hosting ISPs' duties in reducing the abuse of the procedures.

60 The notice-and-takedown procedures in the EU turn out to be very fragmented. Some member states have adopted statutory notice-and-takedown procedures, including Finland, Hungary and Lithuania. Some other member states, such as France, Italy and UK, rule on the elements of a competent notice in their national legislations about implementing E-commerce Directive. There also exist member states which have not ruled on the elements of a competent notice at legislative level, including Holland and Germany. See Sec. 5.2 of this thesis.

Since the Internet is characterized by anonymization, which causes lots of troubles for copyright owners to trace the infringing Internet users, hosting ISPs are obligated to disclose the suspect Internet users' personal identities under the circumstances prescribed by laws. Chapter 6 compares the rules of disclosing Internet users' personal identities in the US, EU and China. By comparison, it summarizes the duties imposed on hosting ISPs by identity disclosure mechanisms in these jurisdictions, and then analyzes the reasonable boundary of these duties.

The disputes between copyright owners and hosting ISPs have not been solved through state regulation, so at a private level, hosting ISPs and copyright owners start to cooperate with each other and reach self-regulation agreements so as to avoid endless lawsuits.[61] Chapter 7 explores two different types of self-regulation, which are codes of conduct and second level agreements reached between hosting ISPs and copyright owners. It first looks into the norms set in codes of conduct and second level agreements, respectively. Then, it evaluates these norms by comparing them with state regulation, and examines whether self-regulation can better preserve hosting ISPs' freedom to operate.

In the conclusion part, chapter 8 summarizes and assesses the research findings in previous chapters, and then answers the questions of how to regulate hosting ISPs' responsibilities for copyright infringement while preserving their maximum freedom to operate in the US, EU and China. By deducing from Chapter 3 and 4, it summarizes how the courts in the US, EU and China decide hosting ISPs' copyright liability under the roof of "safe harbor" provisions, and then suggests how the liability rules ought to be interpreted so as to avoid imposing unreasonable burdens on hosting ISPs. By deducing from Chapter 5 and 6, it summarizes how notice-and-takedown procedures and identity disclosure mechanisms are applied in the US, EU and China, and then suggests how to cast hosting ISPs' duties in these two institutions so as to properly ensure their freedom to operate. By deducing from Chapter 7, it summarizes the advantages and disadvantages of self-regulation, and then answers the question of whether self-regulation can better preserve hosting ISPs' freedom to operate. In addition, it also provides some recommendations for hosting ISPs who are currently conducting business or planning to operate in the US, EU and China. Finally, it addresses the limitations of this research and points out what could be done in the future.

61 Hugenholtz, 'Codes of Conduct and Copyright Enforcement in Cyberspace' (n55), at 303.

Chapter 2

Responsibility Rules of Copyright Enforcement on Hosting Platforms

This chapter introduces the rules related to regulating hosting ISPs' copyright responsibilities. First, this chapter explores the secondary liability rules in the copyright field in the US, EU and China. In the EU, since there is only limited harmonization in respect of secondary liability rules, this chapter looks a little bit further into secondary liability rules in several member states, which lays the basis to discuss the case law in these member states in the following chapters (2.1). Second, this chapter preliminarily explores the liability exemption rules - "safe harbor" provisions in the US, EU and China (2.2). Third, based on the comparison done on liability rules and "safe harbor" provisions, it summarizes the copyright responsibilities that might be imposed on hosting ISPs in the US, EU and China, which provides a basis for the analysis of how these responsibility rules are applied in the following chapters (2.3).

2.1 Secondary Liability Rules in the US, EU and China

Under secondary liability rules, a facilitator who does not commit infringement by itself but merely contributes to the dissemination of infringing materials may be held liable as an indirect infringer.[62] In this respect, hosting ISPs, as facilitators of information transmission on the Internet, may assume secondary liability for the infringing material posted by their subscribers. So far, no relevant rules about indirect infringement have
32 been widely adopted at international level in the area of copyright law.[63] So, each country is substantially free to enact its own domestic norms that regulate indirect infringement of copyright law. As noted by Lynda J. Oswald, because of the lack of harmonization regarding secondary liability rules at international level, businesses face uncertainty to evaluate the infringement liability in other jurisdictions, which "makes it difficult for businesses to effectively plan international intellectual property strategies."[64] In the following text, the secondary liability rules in the US, EU and China are explored and compared.

62 In the US, there are contributory infringement and vicarious infringement. In the UK, there are authorization infringement and joint tortfeasor rules. In France, Germany and China, courts deal with facilitators' liability for copyright infringement by referring to general tort law principles. See the discussion in Section 2.1.1, 2.1.2 and 2.1.3.

63 Berne Convention, Trips Agreement, WCT and WPPT do not provide any rules about indirect copyright infringement. The Free Trade Agreements signed between countries may include some rule regulating indirect copyright infringement, such as Australia revised its Copyright Act in 2004, and brought in the US "safe harbor provision", according to the Free Trade Agreement signed with the US, see Weatherall K, 'Of Copyright Bureaucracies and Incoherence: Stepping Back from Australia's Recent Copyright Reforms' (2007) 31 Melbourne University Law Review 967, at 973-975.

64 Oswald LJ, 'International Issue in Secondary Liability for Intellectual Property Rights infringement' (2008) 45 American Business Law Journal 247, at 248.

2.1.1 Secondary Liability Rules in the US

In the US, where a common law system is adopted, the courts rather than Congress have taken the lead in considering the relevant policies and developing theories of secondary liability.[65] The 1909 Copyright Act did not have any provision addressing liability for indirect infringement.[66] The 1976 Copyright Act still did not explicitly mention indirect infringement or the liability activities that are undertaken by someone other than the direct infringer. However, compared with the 1909 Copyright Act, the 1976 Act not only grants copyright owners the exclusive rights to explore their works, but also adds that copyright owners can authorize others to do so.[67] The legislative history of 1976 Copyright Act indicates that the addition of words "to authorize" as a copyright owner's right in § 106 was intended to confirm congressional intent that secondary or third-party infringers could be liable for copyright infringement in certain circumstances.[68] Congress realized that it is impractical or futile for a copyright owner to sue a multitude of individual infringers, so the law allows a copyright holder to sue a contributor to the infringement instead, in effect for aiding and abetting.[69]

Although the 1976 Copyright Act implies that contributory infringers can be held liable, the Act left the details of the secondary liability doctrines to the courts to apply in specific cases.[70] The US courts have developed two theories of indirect infringement—vicarious liability and contributory infringement based on the second liability rules in tort law.[71] As for vicarious liability, it can be traced back to the "respondeat superior" doctrine developed under the law of agency, which means in certain circumstances, the principal can be held liable for the infringements done by its agent.[72] In the landmark case of *M. Witmark & Sons v. Calloway*, the court held:[73]

Neither does the fact, if it is a fact, that young Williams, the operator of the player piano, borrowed this music without the direction, knowledge, or consent of the owner or manager of the theater affect the question. The rule of common law applies, to wit, that

65 Cohen JE, Loren LP, Okediji RL, O'Rourke MA, *Copyright in A Global Information E*conomy, (Aspen Publisher 2010 (3rd)), at 476.

66 Heath C and Liu KC, *Copyright Law and the Information Society in Asia* (Bloomsbury Publishing 2006), at 229.

67 § 106 of 1976 Copyright Act reads that "the owner of copyright under this title has the exclusive rights to do and to authorize any of the following (exploration)." 1909 Copyright Act reads that "any person entitled thereto, upon complying with the provisions of this Act, shall have exclusive…"

68 Cohen JE, Loren LP, Okediji RL, O'Rourke MA, Copyright in A *Global Information Economy* (n62), at 476.

69 *In re Aim*ster *Copyright Litigation*, 334 F.3d 643 (7th Cir. 2003), at 646.

70 Statement of Marybeth Peters, The Register of Copyrights before the Committee on the Judiciary (Intentional Inducement of Copyright Infringements Act of 2004), United States Senate, 108th Congress, 2nd Session, July 22, 2004.

71 Batholomew M and Tehranian J, 'Secret Life of Legal Doctrine: The Divergent Evolution of Secondary Liability in Trademark and Copyright Law' (2006) 21 Berkeley Technology Law Journal 1363, at 1366.

72 Nimmer D, *Nimmer on Copyright*, §12B.04[A][1], (LexisNexis, 2013) 12.04 [A] [2].

73 *M*. W*itmark & Sons v. Calloway*, 22 F.2d 412 (D. Tenn. 1927), at 415, quoting *Merges RP, et al., Intellectual Property in the New Technological Age: Case and statutory supplement* (Aspen Law & Business. 2005), at 570.

the master is civilly liable in damages for the wrongful act of his servant in the transaction of the business which he was employed to do, although the particular act may have been done without express authority from the master, or even against his orders.

Eventually, vicarious liability goes beyond the master-servant context, and extends liability to those who profit from infringing activity where they have the right and ability to prevent infringement.[74] As noted by Nimmer, the owner of a dance hall may need to undertake vicarious liability for infringing performances of the orchestra, even if the orchestra is hired as an independent contractor and exclusively determines the music to be played.[75] Basically, vicarious liability does not require the defendant to know the tortious act, but rather, the liability is rendered on the defendant strictly because of his or her relationship with the direct tortfeasor.[76] In order to find vicarious liability, two elements need to be present. First, the defendant must possess the right and ability to supervise the infringing conduct. Second, the defendant must have "an obvious and direct financial interest in the exploitation of copyrighted materials."[77]

Contributory infringement also finds its theoretical basis in tort law, particularly the principle of joint and several liability.[78] As defined in case law, a party "who, with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct of another, may be held as a contributory infringer."[79] By following this logic, in the case of *Elektra Records v. Gem Elec. Distribs*, the defendant
34 who sold blank tapes and made available both pre-recorded tapes of copyrighted works and a high speed, coin-operated "Make-A-Tape" system, was eventually held contributorily liable for the infringing copies made by its customers.[80] Therefore, if there is knowledge that the work in question constitutes an infringement, then the one who causes another to infringe will himself be liable as an infringer.[81] Further, "in order to be deemed as a contributory infringer, the authorization or assistance must bear some direct relationship to the infringing acts, and the person rendering such assistance or giving such authorization must be acting in concert with the infringer."[82] Just as described by the Supreme Court, a contributory infringer is someone who "was in a position to control the use of copyrighted works by others and had authorized the use without permission from the copyright owner."[83]

74 Ibid.
75 Nimmer D, *Nimmer* on *copyright* (n85),§12B.04[A][1], 12.04 [A] [2].
76 Batholomew and Tehranian, 'Secret Life of Legal Doctrine: The Divergent Evolution of Secondary Liability in Trademark and Copyright Law' (n68), at 1366.
77 Nimmer D, *Nimmer on copyright* (n85),§12B.04[A][1], 12.04 [A] [2].
78 See Cohen, Loren, Okediji and O'Rourke, *Copyright in A Global Information Economy* (n62), at 476.
79 *Gershwin Publishing Corp. v. Columbia Artists Management, Inc.*, 443 F.2d 1159 (2d Cir. 1971).
80 *Elektra Records v. Gem Elec. Distribs*, 360 F. Supp. 821 (E.D.N.Y 1973). Quoting Merges, et al., *Intellectual Property in the New Technological Age: Case and Statutory Supplement* (86), at 571.
81 Nimmer D, *Nimmer on copyright* (n85),§12B.04[A][1], 12.04 [A] [3][a].
82 Ibid.
83 *Sony Corp. of America v. Universal City Studios, Inc.* (n27), at 437.

Regarding copyright protection, contributory infringement and vicarious liability, to some extent, complement each other. Someone who has no knowledge of a third party's infringement, cannot be held liable for contributory infringement. By contrast, he may need to undertake vicarious liability, if he has right and ability to control infringement and directly benefits from it.[84] Conversely, in various circumstances, vicarious liability will be absent because of the lack of supervision of the infringing activities or of a direct financial interest in the infringing activities, but third party liability may still exist via contributory infringement, if the defendant acts with knowledge and his activities aid the primary infringer in accomplishing his illegitimate activity.[85]

2.1.2 Secondary Liability Rules in the EU

At the EU level, no explicit provision has been enacted to define under what circumstances a defendant should be secondarily liable for copyright infringement, and relevant EU directives only indicate that an injunction relief can be issued against intermediaries if their services are used by third parties for infringing purposes.[86] According to the EU Copyright Directive, "Member States shall ensure that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right."[87] In this respect, the EU law seems to contain "a minimum nucleus of secondary liability" for copyright infringement, and that is the general possibility to request injunctions against intermediaries.[88] Nevertheless, the Copyright Directive does not provide the explicit rules about the injunction relief, but only states that, "without prejudice to any other sanctions and remedies available, the right owners should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in an internet…. The conditions and modalities relating to such injunctions should be left to the national law of the Member States."[89] Therefore, even the "minimum nucleus of secondary liability" is mainly left for the Member States to decide its conditions and procedures at their discretion. Further, the crucial question of secondary liability, which is about whether, or under which conditions, copyright

84 Nimmer D, *Nimmer on copyright* (n85),§12B.04[A][1], 12.04 [A] [3][a].

85 Ibid.

86 Council Directive 2001/29/EC of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society [2001] OJ L 167/10, Art. 8(3); Council Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights [2004] OJ L 195/16, Art. 11.

87 Ibid, Directive 2001/29/EC, Art. 8(3). The Article 11 of Directive 2004/48/EC directly refers to the Article 8(3), and reads that "Member States shall also ensure that rights holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC."

88 Leistner M, 'Structural aspects of secondary (provider) liability in Europe' (2014) 9 Journal of Intellectual Property Law & Practice 75, at 76.

89 Directive 2001/29/EC (n83), Recite 59.

owners can claim damages against indirect infringers, is also left for Member States to regulate.[90] As mentioned in the Introduction, since the courts in Germany, France, the UK and Italy have developed some specific rules that regulate hosting ISPs' copyright liability, Chapter 3 and 4 choose these four member states to do a case law study. Therefore, the following text only looks into the secondary liability rules regarding copyright infringement in these four Member States.

2.1.2.1 German Laws

Article 97 of the German Act on Copyright and Related rights provides as follows: "1) any person who infringes copyright or any other right protected under this Act may be required by the injured party to eliminate the infringement or, where there is a risk of repeated infringement, may be required by the injured party to cease and desist. Entitlement to prohibit the infringer from future infringement shall also exist where the risk of infringement exists for the first time. 2) Any person who intentionally or negligently performs such an act shall be obliged to pay the injured party damages for the prejudice suffered as a result of the infringement …." From this provision, there is not any obvious clue about indirect liability for copyright infringement. But according to an established formulation in case law, anyone who has in any way whatsoever willingly provided cause on the part
36 of others can essentially be held responsible.[91] From this broad understanding, all forms of participation are covered, ranging from complicity to indirect delinquency, up to inducement and contributory infringement.[92]

Actually, the abovementioned Article 97 can trace its origin back to Article 823 and Article 1004 of German Civil Law. In the light of Article 823 of German Civil Law, the imputed fault should be found so as to ask someone to undertake liability.[93] When deciding imputed fault, "duty of care" is an important notion to be referred to. Principally, if anyone through its activity or property creates a source which may put others' rights and interest in potential danger, a duty of care will be provoked, which also includes a duty to prevent a third party's misuse of its property to infringe other's rights.[94] Therefore, a hosting ISP may be liable, if someone takes advantage of its service to commit infringements. As to draw a borderline for the duty of care, the advantages of maintaining a source of danger is usually weighed against potential damages to the other's rights so as to reach a proper duty scope.[95]

90 Leistner, 'Structural aspects of secondary (provider) liability in Europe' (n85), at 76.

91 Spindler G and Leistner M, 'Secondary copyright infringement-New perspectives in Germany and Europe' (2006) 37 International Review of Intellectual Property and Competition Law 788, at 794.

92 Ibid.

93 German Civil Code, Section 823(1).

94 Angelopoulos C, 'Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe' (2013) 3 Intellectual Property Quarterly 253, at 267.

95 Ibid.

Moreover, Article 1004 of the German Civil Law prescribes a liability called "stoererhaftung" (disturber's liability), which has been developed into the main tool for German courts to deal with the secondary liability of Internet platforms for copyright infringement.[96] This liability rule is only focused on claims for injunction and removal rather than claims for damages.[97] Generally, the following three requirements need to be fulfilled so as to trigger disturber's liability: 1) the disturber contributes to the infringement of protected rights and this contribution is the causation of the infringement from a legal perspective; 2) the disturber should have the capacity to prevent the primary infringement; 3) the disturber should have already breached the reasonable duty of care he needs to undertake.[98] To be mentioned, disturber's liability can be concluded without considering the disturber's negligence or whether the direct infringer or intentional contributor has been sued.[99]

Besides, Article 830 of the German Civil Code also opens a door for regulating indirect infringements, which provides that where through a jointly committed unlawful action several persons cause damages, each of these people is responsible for such damage; and the persons who induce or contribute to the action should be seen as joint infringers.[100] In the application of this provision, the courts assess whether the defendant has induced or contributed to the infringement, considering the defendant's intention, whether there is knowledge of the infringing circumstances, the degree of control exercised by the defendant, whether or to what extent the defendant has a duty to monitor his activities and whether the defendant is guilty of reckless conduct or has created a dangerous situation.[101]

Therefore, with the absence of clear regulations about indirect infringement in Copyright Law, the German courts hear relevant cases based on doctrines of German general tort law, and a series of case laws have been developed following this track. Under these case laws, the event organizers may be held liable, if the copyrighted works are performed without legal permission; and the providers of products and infrastructure with whose help copyright infringement may be undertaken, may be liable as indirect infringers.[102] Besides, some new concepts were created during the developing process of case law, such as supervision, control and inspection duties; however, these duties as preconditions of secondary infringement have not yet been related to the classic elements of a general tort action under

96 Leistner, 'Structural aspects of secondary (provider) liability in Europe' (n85), at 78.

97 Jan Bernd Nordemann, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in Germany' in Heath C and Sanders AK eds., *Intellectual Property Liability of Consumers, Facilitators, and Intermediaries* (Kluwer Law International 2012), at 47.

98 Ibid, at 47-48.

99 Ibid.

100 Sterling, JAL, *World Copyright Law*, (Sweet & Maxwell. 2008), at 629.

101 Ibid.

102 See Spindler and Leistner 'Secondary copyright infringement-New perspectives in Germany and Europe' (n88), at 798-801.

German law.[103] Hence, the question as to whether the supervision, control and inspection duties of the operator correspond to the element of unlawfulness (Rechtswidrigkeit), the element of negligence (verschulden) or the question of responsibility for another person (zurechnung), has not been answered clearly by the courts.[104] Nevertheless, according to Gerald Spindler and Matthias Leistner, the latest developments in case law gave rise to a doctrine that attempts to relate secondary infringement concepts in intellectual property and unfair competition law to the corresponding rules on indirect liability in general tort law, so as to re-integrate the case law concepts from intellectual property into the traditional principles of general tort law.[105]

2.1.2.2 *French laws*

French intellectual property code focuses on stricter IP enforcement, and offers few clues about indirect copyright infringement.[106] Furthermore, in the area of copyright, the Court of Cassation concluded that, since copyright was an exclusive right, no fault was needed to impose both of injunction relief and damage payment on the infringer, which can be called strict liability.[107] The Court of Cassation's decision may justify setting a strict liability against the primary offender, but regarding the "multiple actors involved in the digital dissemination of works who
38 do not contribute an infringement and whose fault is harder to take as given," it seems unfair to impose a strict liability.[108] Therefore, as what occurs in Germany, the French courts hear the cases about indirect copyright infringement on the basis of general tort doctrines provided in French Civil Code, under which the fault is required for imposition of damage payment.[109] Article 1382 of French Civil Code provides that "any act whatever of man, which causes damage to another, obliges the one by whose fault it occurred, to compensate it;" and Article 1383 provides that everyone is liable for the damage he causes not only by his intentional act, but also by his negligent conduct or by his imprudence.[110] Therefore, under French law, the secondary liability may arise if someone willfully or negligently causes the

103 Ibid, at 802.
104 Ibid.
105 Ibid, at 794.
106 Nérisson S, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in France' in Heath C and Sanders AK eds., Intellectual Property Liability of Consumers, Facilitators, and Intermediaries (Kluwer Law International 2012), at 68.
107 Angelopoulos, 'Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe' (n91), at 260.
108 A Lucas & H-J Lucas, Traité de la Propriété Littéraire et Artistique, (2nd ed, Litec 2001) 606 et seq. quoting Angelopoulos, ibid.
109 Leistner, 'Structural aspects of secondary (provider) liability in Europe' (n85), at 86.
110 Edward A Tomlinson, Tort Liability in France for the Act of Things: A Study of Judi*cial Lawmaking*, 48 La. L. Rev. (1987). 1361.

copyright infringement conducted by a third party.[111] When defining the "willful" or "negligent" causation, French courts always refer to the important notion - reasonable duties of care in general tort law.[112] Therefore, if a defendant is held as not fulfilling reasonable duties of care to prevent a third party from committing copyright infringement in question, he probably needs to be liable.[113] In fact, before the specific legislation about hosting ISPs' liability was adopted, French courts usually decided hosting ISPs' liability by referring to the aforesaid liability rules.[114] For instance, in the Lacoste case, based on the general duty of care provided in Article 1382 and Article 1383 of Civil Code, the High Court of Nanterre set three specific duties on service providers: to call the users' attention to respect the rights of others, to undertake professional care against infringement, to remove the verified unlawful materials and prevent them from being reposted.[115] Later, the Court of Appeal of Versailles further held that the duty of care should not require a hosting ISP to undertake a general and systematic monitoring on all content on its platform, but only "due diligence checks (diligences approprieés)," which can be provoked "once it acquires knowledge of the unlawful nature of the content on a site or once it has reason to suspect unlawfulness."[116]

In order to promote freedom of speech, French law limits the liability of specific facilitators of transmitting information, such as editors and publishers, so as to encourage them to disseminate works.[117] If the editors and publishers can reveal the contact information or identities of the authors of works to the claimants, they do not need to be liable for the infringing contents they have published.[118] The French law makers tried to extend this legal principle into the digital transmission of information on the Internet. In terms of "Freedom of Communication Act," hosting ISPs need to keep the identification information of the users who publish the contents on their platforms so as to avoid being liable for the infringement committed by their users.[119] In this respect, the facilitators of information transmission can avoid being secondarily liable, as long as they can help the claimants identify the direct infringers. However, unlike in the physical world where publishers usually keep sufficient identity data, the data retained by hosting ISPs is normally not explicit

111 Leistner, 'Structural aspects of secondary (provider) liability in Europe' (n85), at 87.
112 Ibid.
113 Ibid.
114 Angelopoulos, 'Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe' (n91), at 264.
115 Madame L. c/ les sociétés Multimania, Tribunal de Grande Instance de Nanterre, 8 December 1999. Quoting Angelopoulos, ibid.
116 S.A Multimania Production c/ Madame Lynda L., Cour d'Appel de Versailles, Arrêt du 8 juin 2000. Ibid.
117 Nérisson, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in France' (n103), at 68.
118 Ibid.
119 Ibid, at 69.

enough to identify the direct infringers.[120] Therefore, this sort of liability privilege in fact may be not quite applicable to hosting ISPs.

2.1.2.3 *Italy laws*

In Italy, Copyright Law does not include any clause about indirect copyright infringement, so Italian courts mainly rely on the vicarious liability or the general principles of civil liability to decide the case about indirect copyright infringement.[121] In the light of Article 2043 of Italian Civil Code, "any act committed either with intent or with fault causing an unjustified injury to another person obliges the person who has committed the act to compensate damages," which provides a legal basis for any person to bring actions for damages.[122] In the case of *PFA Films v. Yahoo*, the District Court of Roma held that as suggested by previous case law, the principles of civil liability which focuses on analyzing the duty of care imposed on the third party, could be applied for deciding indirect copyright infringement on the Internet.[123] Besides, according to Article 2055 of the Italian Civil Code, "if more than one person is accountable for the violation of someone's right, they are jointly liable for compensation and damages." [124] Although there does not seem to be any case law or literature on the concept of contributory infringement in the context of copyright law related to the Internet, it would be unwise to assume that
40 contributory infringement in Internet cases would not be covered by the general principle set forth in Article 2055 of the Italian Civil Code.[125]

2.1.2.4 *UK laws*

The UK Copyright Designs and Patents Act 1988 (CDPA) provides a special section called "secondary infringement of copyright", according to which, certain acts, including importing infringing copy, possessing or dealing with infringing copy, providing means for making infringing copy and so on, will constitute infringement if the defendant knows or has reason to believe that an infringing copy is involved. [126]

120 In the case of *Dargaud Lombard and Lucky Comics v. Tiscali Media*, the court, under the claim of two plaintiffs, requested Tiscali – a hosting ISP – to disclose the identity data of its subscriber who uploaded the infringing content, but Tiscali could only communicate the registration data, such as last name and first name: "comics", address: "comics street", and so on, which were totally unreliable for identifying the suspected subscriber. See ibid, at 77.

121 Barazza S, 'Secondary liability for IP infringement: converging patterns and approaches in comparative case law' (2012) 7 Journal of Intellectual Property Law & Practice 879, at 882.

122 Maggiore M and Tardella E, 'Study on the conditions of claims for damages in case of infringement of EC competition rules – National Reports (Italy)' (2012), European Commission, at 3.

123 Barazza, 'Secondary liability for IP infringement: converging patterns and approaches in comparative case law' (n118), at 882.

124 Köhler C and Burmeister K, 'Copyright liability on the Internet today in Europe (Germany, France, Italy and the E.U.)' (1999) 21 European Intellectual Property Review 485, at 491.

125 Ibid.

126 See UK Copyright, Designs and Patents Act 1988, Section 22 to Section 26.

Therefore, when deciding the secondary infringement of copyright, it is important to examine whether the defendant knows that he is dealing with infringing copy.[127] However, the secondary infringement of copyright only applies to the five acts prescribed by CDPA Section 22-26, which do not particularly fit into establishing third party liability in online context.[128]

Nevertheless, the authorized copyright infringement provided for in Section 16(2) offers an important reference for indirect infringement, according to which, since copyright owners have exclusive right to authorize others to use their works, copyright in a work is infringed by a person who without permission of the copyright owner, authorizes another to do any of the acts restricted by the copyright.[129] Although the unlawful authorization is categorized as primary infringement in the UK Copyright Act, but in light of the common understanding, it covers both direct infringement and indirect infringement in the copyright area,[130] since "over time the concept of authorization has evolved to exact liability beyond the directly and vicariously liable, from persons associated or affiliated in a variety of ways with the primary infringer."[131] Regarding the authorized infringement, it's very important to define what constitutes "authorize". In terms of the case law, authorize means, "sanction, approve, countenance".[132] To be more detailed, if a defendant is confirmed to have committed authorized infringements, at least, he has some ability to control or prevent the infringing act, and also has some degree of knowledge of the infringements or the circumstances including the likelihood that infringement will be done.[133] In a common sense, the term "authorization" can be literally understood as requiring some degree of authority, so mere facilitation should be excluded from authorization of copyright infringement.[134] Similarly, regarding the online technologies which are "by their nature almost inevitably to be used for the purpose of an infringement," since the law does not prohibit their invention, manufacture, sale and advertisement, running such online technologies cannot be naturally concluded as authorization of infringement.[135]

127 Llewelyn D, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: Concepts under Common Law' in Heath C and Sanders AK eds., *Intellectual Property Liability of Consumers, Facilitators, and Intermediaries* (Kluwer Law International 2012), at 21.

128 Bently L and Sherman B, *Intellectual property law* (Oxford University Press. 2014), at 220.

129 UK Copyright, Designs and Patents Act 1988 (n123), Section 16 (2).

130 Gendreau Y, 'Authorization revisited' (2000) 48 Journal of the Copyright Society of the U.S.A. 341, at 341. Llewelyn, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: Concepts under Common Law' (n124), at 22. Hocking R 'Secondary liability in copyright infringement: still no Newz?' (2012) 23 Entertainment Law Review 83, at 83.

131 Angelopoulos, 'Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe' (n91), at 256.

132 *Falc*on *v. Famous Players Film Company* [1962] 2 K.B. 474 at 491.

133 See Jane G Ginsburg and Sam Ricktson, Inducers and Authorisers: A comparion of the US Supreme Court's Grokster decision and the Australian Federal Court's KaZaa ruling, 11 Media & Art Law Review, Vol. 11, No. 1, 2006.

134 See C*BS Inc v. Ames Records and Tapes* [1981] 2 All ER 812.

135 Angelopoulos, 'Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe' (n91), at 258.

In order to provide a degree of legal certainty about liability for authorizing infringements, in Australia, the Copyright (Digital Agenda) Amendment Act 2000 provides some factors for courts to decide authorizing infringement,[136] and these factors were also cited by the UK court in the landmark case "Newzbin".[137] These factors are as follows: "a) the extent (if any) of the person's power to prevent the doing of the act concerned; b) the nature of any relationship existing between the person and the person who did the act concerned; c) whether the person took any reasonable steps to prevent or avoid the doing of the act, including whether the person complied with any relevant industry codes of practice."[138]

Further, according to the common law, an intermediary may attract liability as joint tortfeasor.[139] In the copyright field, the basic principles of joint tortfeasance were laid down in the two Amstrad cases.[140] In these two cases, Amstrad produced and sold the machines consisting of a radio, a gramophone and a tape recorder with "two cassette decks" which allowed users to record from tape to another, and in the advertisements Amstrad also propagated the recording capacity of the machines.[141] The debating issue is whether Amstrad should be held as a joint tortfeasor, since the machines could be used by consumers for making illegal copies. The court held that, "a defendant who procures a breach of copyright is liable jointly and severally with the infringer for the damages suffered by the plaintiff as a result of the infringement;
42 the defendant is a joint infringer if he intends and procures and shares a common design that infringement shall take place; a defendant may procure an infringement by inducement, incitement or persuasion."[142] So, joint tortfeasance can be found, if a defendant procures the breach of copyright or commits infringement in common design with others. Since the machines sold by Amstrad were capable of being used for lawful and unlawful purposes, and the consumers independently decided how to use the machine, no common design could be found.[143] Regarding procurement, although Amstrad's machine could be used for dual purposes and its advertisement might persuade consumers to buy the machines because of their capacity for making illegal copies, Amstrad did not procure the infringement, since the advertisement would not "influence the purchaser's later decision to infringe copyright."[144]

136 Australia Copyright Act 1968, Sec. 36 (1A), and Sec. 101(1).

137 *Twentieth Cen*tury *Fox Film Corp v. British Telecommunications Plc*, Royal Courts of Justice, [2011] EWHC 1981 (Ch). Para. 91.

138 Australia Copyright Act 1968, Sec. 36 (1A) and Sec. 101(1).

139 Llewelyn, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: Concepts under Common Law' (n114), at 24.

140 Leistner, 'Structural aspects of secondary (provider) liability in Europe' (n85), at 82. These two cases are as follows: *Amstrad Consumer Electronics PLC v. The British Phonographic Industry Limited* [1986] FSR 159; *CBS songs ltd and others v Amstrad Consumer eElectronics PLC and other* [1988] 2 WLR 1191.

141 Ibid.

142 Ibid.

143 Ibid.

144 Ibid.

> In the view of Lord Templeman, procurement, whether by inducement, incitement or persuasion, must be directed to "an individual and must identifiably procure a particular infringement in order to make the defendant liable."[145]

To sum up, since there is only limited harmonization regarding indirect copyright infringement in the EU, the member states develop their own approaches to deal with indirect copyright infringement. In the EU, the member states such as Germany, France and Italy do not provide any specific rules about indirect infringement in their copyright laws, and the courts mainly rely on the liability principles, particularly the duty of care notion, in civil laws to deal with indirect copyright infringement. In the UK, although CPDA includes a specific section called "secondary infringement of copyright", whether an intermediary is secondarily liable mainly depends on how to apply the rules about authorization infringement and joint tortfeasance.

2.1.3 Indirect Infringement Rules in China

Article 46 of the Chinese Copyright Law provides a list of conducts which constitute copyright infringements, but none of the listed conducts can be referred to an indirect infringement.[146] Therefore, just as the other countries belonging to a civil law system, the courts in China also refer to general tort law doctrines to address copyright indirect infringements. According to Article 130 of the General Principles of Civil Law, two or more than two persons who cause damage to others by joint infringement, will assume liability jointly. As for what constitutes joint infringement, the Supreme People's Court[147] declared that, a person who instigates or assists others to perform an infringement shall be the co-infringer, and will assume civil liabilities jointly.[148] In the field of Internet copyright, the Supreme People's Court follows the same track, providing that, if an internet service provider who participates in copyright infringements made by others, or instigates or assists others to conduct copyright infringements on the internet, the people's courts should, in term of

145 Ibid.

146 Standing Committee of the National People's Congress (全国人民代表大会常务委员会), Copyright Law of the People's Republic of China (中华人民共和国著作权法), Order No. 26 of the President of the People's Republic of China (中华人民共和国主席令第二十六号), February 26, 2010, Art. 46.

147 In China, Supreme People's Court is authorized to deliver interpretation on the questions involving the application of laws and decrees. See Standing Committee of the National People's Congress (全国人民代表大会常务委员会), Resolution of the Standing Committee of the National People's Congress Providing an Improved Interpretation of the Law (全国人民代表大会常务委员会关于加强法律解释工作的决议) , Adopted at the 19th Meeting of the Standing Committee of the Fifth National People's Congress, June 10, 1981, Art. 2. The interpretations delivered by Supreme People's Court are named as "Judicial Interpretations" (司法解释) which constitute one source of law in China.

148 Supreme People's Court (最高人民法院), Opinions of the Supreme People's Court on Certain Issues Concerning the Implementation of the "General Principles of the Civil Law of the People's Republic of China" (Trial) (最高人民法院关于贯彻执行《中华人民共和国民法通则》若干问题的意见（试行）), Fa (Ban) Fa [1998] No. 6 (法(办)发[1998]6号), January 26, 1988, Art. 148.

Article 130 of "General Principles of Civil Law", confirm that, the internet service provider undertakes joint liability with other conductors or the persons committing infringement directly.[149] If the Internet Service Provider who serves contents to the public[150], actually knows that its subscriber is committing copyright infringements on the Internet, or after receiving the evidently warning notices pointing to infringements, but still does not remove infringing contents or take any other measures to eliminate the infringements, the people's courts should hold that, the Internet service provider undertakes joint and several liability with its subscriber according to Article 130 of "General Principles of Civil Law".[151] So in China, if accusing an ISP of committing indirect infringement, the ISP must be found to actually be aware of or at least should know (but doesn't know because of negligence) the direct infringement made by others. In 2009, the China Tort Law was enacted and promulgated by the Standing Committee of the National People's Congress. Because when China Tort Law was still in drafting, there were lots of cases in which the ISPs' services were used for defamation, copyright infringement and trademark infringement, the legislators in China felt that it was necessary to draft a specific provision on ISPs' liability. According to Article 36, if an Internet user commits a tort through the Internet services, the victim of the tort should be entitled to notify the Internet service provider to take such necessary measures as deletion, blocking or disconnection.[152] If, after being notified, the Internet service provider fails to take necessary measures in a timely manner, it shall be jointly and severally liable with the Internet user for any additional damages.[153] Where an Internet service provider knows that an Internet user is infringing upon a civil right or interest of another person through its Internet services, and fails to take necessary measures, it will be jointly and severally liable with the Internet user for any additional damages.[154] Therefore, whether an ISP should be secondarily liable depends on whether it knows of the infringement committed by its users. When deciding whether an ISPs should know of the infringement, the courts in China also refer to the duty of care notion based in general tort rules.[155]

149 Supreme People's Court (最高人民法院), Interpretation of the Supreme People's Court on Certain Issues Related to the Application of Law in the Trial of Cases Involving Computer Network Copyright Disputes (最高人民法院关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释) (thereafter "Internet Interpretation (2006)"), Fa Shi [2006] No. 11 (法释[2006]11号), November 22, 2006, Art. 3.

150 The Internet service provider who serves content to the public points at the websites offering storage space for their subscribers to upload contents on the Internet, but doesn't mean it offers content to the public directly.

151 Internet Interpretation (2006) (网络解释(2006)) (n145), Art. 4.

152 Standing Committee of the National People's Congress, Tort Law of the People's Republic of China (中华人民共和国侵权责任法) (thereafter China Tort Law), Order of the President of the People's Republic of China No. 21 (中华人民共和国主席令第二十一号), December 29, 2009, Art. 36.

153 Ibid.

154 Ibid.

155 Wu HD(吴汉东), 'Study on Internet Service Providers' Liability for Copyright Infringement (论网络服务提供者的著作权侵权责任)' (2011) 2 China Legal Science (中国法学) 38, at 38-47.

> If an ISP has already fulfilled reasonable duty of care to prevent infringement from occurring, it would be held to be unaware of the infringement, and otherwise it would be held to be aware of the infringement.[156]

Based on the discussion above, it can be found that the secondary liability rules in the copyright field are quite diverse in the US, EU and China. For instance, in the US, the issue of indirect copyright infringement is dealt with under contributory infringement and vicarious liability developed from case law. In the EU, since there is only limited harmonization with regard to indirect copyright infringement at the EU level, member states are allowed to establish their own secondary liability rules in their national laws. In the UK, whether an intermediary commits an indirect copyright infringement is mainly decided under authorizing infringement and joint tortfeasance theories. In other member states, where a civil law system is adopted, such as Germany, France and Italy, the courts mainly hear the cases about indirect copyright infringement by referring to general tort rules in civil codes, particularly the duty of care notion. In China, since the Tort Law was enacted in an era where infringement occurs so frequently on the Internet, it includes a specific Article that regulates ISPs' secondary liability. Nevertheless, when Chinese courts interpret this specific Article, they also refer to the duty of care notion. Therefore, in these civil law countries, duty of care plays an important role in determining whether a defendant is an indirect copyright infringer. In Chapters 3 and 4, the case law will demonstrate how courts shape hosting ISPs' secondary liability by referring to the liability rules discussed above.

2.2 "Safe Harbor" Provisions

The previous section explored the secondary liability rules regarding copyright infringement in the US, EU and China. This section will discuss the liability exemption rules that are particularly granted to ISPs. As referred to in the first chapter, for the purpose of preserving the freedom to operate of hosting ISPs, "safe harbor" provisions have been adopted in the US, EU and China. In the light of "safe harbor" provisions, hosting ISPs can be exempted from undertaking monetary liability under qualified circumstances.[157] Besides, liability exemption rules, "safe harbor" provisions also include notice-and-takedown procedures and identity disclosure mechanisms, which impose certain obligations on hosting ISPs to help copyright owners enforce their copyright against infringement. In the following section, the "safe harbor" provisions in the US, EU and China will be introduced and compared.[158]

156 Ibid.

157 See DMCA (n1), Sec. 512 (c)(1); E-commerce Directive (n1), Art. 14; Internet Regulation (信息条例) (n1), Art. 22.

158 This section aims at providing readers with a general frame of liability exemption rules in the US, EU and China, and how these rules are applied will be discussed in Chapter 3, 4, and 5.

In the EU, because of the existence of the E-commerce Directive, "safe harbor" provisions have reached a sort of harmonization in member states.[159] Therefore, this section only discusses the "safe harbor" provisions in the E-commerce Directive, instead of looking further into "safe harbor" provisions in Member States.

2.2.1 US DMCA §512

In 1998, the US congress enacted the Digital Millennium Copyright Act ("DMCA"), which aims to solve the challenges presented by the rapid expansion of the Internet. Section 512 of DMCA exempts four categories of ISPs from monetary remedies if their acts follow the requirements listed by this section. DMCA §512 provides a broad definition of "a provider of online service or internet access, or the operator of such facilities", so the services, such as providing internet access, e-mail, chat room and web page hosting services, are all included.[160] Furthermore, based on different characteristics of various services operated by ISPs, the DMCA §512 provides different requirements for each safe harbor.

The DCMA 512 (a) provides safe harbor for "conduit", which offers Internet access service to the public to transmit information on the Internet, such as AOL in the US. For this kind of ISP, it can enjoy exemption from monetary damages for its subscribers' copyright infringements, if the following requirements are met: 1) the transmission of
46 the material is initiated by a third party; 2) the whole process of transmission is carried out automatically and without selection and modification of the material by the ISP; 3) the ISP does not select the recipients; 4) no copy is maintained on its system longer than necessary and can not be accessed by others than the targeted recipients.[161]

The second safe harbor is conferred to the kind of storage called "caching", which is used to increase Internet performance and to reduce Internet congestion. The exempting conditions to be met by ISPs offering a caching service generally reflect those specified in the previous safe harbor, such as the material is made available online by a third party and transmitted at the direction of another third party, and storage is carried out through an automatic technical process without modification to its content.[162] Besides, if the person making material available online changes the content of the material, the copy stored in caching also needs to be refreshed, reloaded or updated through an automatic technical process, and the caching ISPs need to follow "notice-and-takedown" procedure.[163]

159 After the enactment of E-commerce Directive (E-commerce Directive), Germany, France, Italy and UK have already implemented the Directive into their domestic laws, see Telemediengesetz (TMG), Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (thereafter LCEN), The Electronic Commerce (EC Directive) Regulations 2002. There are some differences between the "safe harbor" provisions in each member states, which will be discussed in Chapter 3 and Chapter 4.

160 H.R. REP. 105-551 (II) (n16), at 64.

161 See DMCA (n1), Sec. 512 (a).

162 Ibid. Sec. 512 (b).

163 Ibid.

The third safe harbor is designed for the so-called "host", which offers Internet storage space for its users to upload their materials.[164] The elements listed by this safe harbor originate from the indirect infringement theories in common law. First, the ISPs does not have actual knowledge that the material or an activity using the material on the system or internet is infringing; in the absence of such actual knowledge, it is not aware of facts or circumstances from which infringing activity is apparent; or upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material.[165] Second, the ISP does not receive a financial benefit directly attributable to the infringing activity, in a case in which the ISP has the right and ability to control such activity.[166] Third, the ISPs need to abide by "notice-and-takedown" procedure, which means upon receiving the competent notification claiming infringement, ISP must respond expeditiously to remove, or disable access to, the material claimed to be infringing or to be the subject of infringing activity.[167]

The fourth safe harbor relates to information location tools such as online directories and hyperlinks, which may refer or link a user to sites that contain infringing materials.[168] In this case, the operator of information location tools should qualify with the same exempting requirements as those listed in the last safe harbor for hosting ISPs.[169]

From reading the requirements of the safe harbor provisions, ISPs have to be passive in the process of transmitting information. For the "conduit" and "caching", the ISPs should keep extremely passive, and what they can do is transmitting information at the direction of their users without choosing what is to be transmitted and to whom the material is transmitted by them. For the "host" and "information location tool", the ISPs also need to play a passive role, but upon finding the apparent infringements or receiving notice claiming infringements, they need to remove or disable the access to these materials on suspicion of infringements.[170]

The "notice-and-takedown" system, as a creative mechanism aiming at fighting against copyright infringement on the Internet, has been designed in detail under DMCA §512. In the case of *Netcom*, which is one of the most important cases between ISP and copyright owner before DMCA §512 was born, the judge required that Netcom establish a written procedure for the handling of future complaints of copyright violation,[171] which was the miniature of the so-called "notice-and-takedown" system in DMCA 512. As provided in the "notice-and-takedown"

164 Ibid, Sec. 512 (c)(1).
165 Ibid, Sec. 512 (c)(1)(A).
166 Ibid, Sec. 512 (c)(1)(B).
167 Ibid, Sec. 512 (c)(1)(C).
168 Sullivan ER, 'Lost in Cyberspace: A Closer Look at ISP Liability' (2001) 12 Entertainment Law Review 192, at 192.
169 See DMCA (n1), Sec. 512 (d).
170 As being discussed in Chapter 3, how to define "passivity" is an important mission for courts, because it decides whether a hosting ISP can enter into "safe harbor".
171 Cunard J and Wells A, The Evolving Standard of Copyright Liability Online (1997) 497 PLI/Pat 365, at 380.

system, the ISP must designate an agent to receive notice of infringements claims, and make the contact information of this agent easily accessible to the public; the notice for claiming infringements should meet certain requirements, particularly sufficient for the ISP to locate the claimed infringing materials; after receiving valid notice, the ISP should remove or disable the access to the materials which are the subject of the infringement claim, and then notify the user who uploads these materials that they will be deleted; upon receiving this notification, the user can send a counter-notice to the ISP denying the infringement, and then the ISP should restore the materials that had been deleted.[172] During this process, the ISPs still play a passive role, because they only need to follow the instruction of the notice without checking the soundness of the notice, and they are also exempt from liability if they make a wrong deletion or restoration by following a notice they have received.[173]

The copyright owners also can apply for a subpoena from the U.S. courts to request ISPs to disclose sufficient information for them to identify the alleged infringers before they launch the lawsuits.[174] Besides, in order to enjoy the exemption from monetary relief, the ISPs should terminate the accounts of subscribers who commit infringements repeatedly, and accommodate but not interfere with the standard technical measures.[175] Last but very important, the ISPs are not obligated to monitor their service or deliberately seek acts indicating infringing activities except to the extent consistent with a standard technical measure,[176] which works as a basis for courts to interpret the other elements about liability exemption listed by DMCA §512.

48

2.2.2 The EU E-commerce Directive

Before the EU Parliament passed a Directive providing "safe harbor" for ISPs, the German Teleservices Act already provided liability limitations for ISPs in certain circumstances as following: providers will not be responsible for any third-party content which they make available for use unless they have knowledge of such content and are technically able and can reasonably be expected to block the use of such content; providers will not be responsible for any third-party content to which they only provide access, and the automatic and temporary storage of third-party content due to user request will be considered as providing access.[177] In the later EU Directive, we can still find traces of the German Teleservices Act.[178]

172 DMCA (n1), Sec. 512 c (3) and g.

173 Ibid, how the notice-and-takedown procedure works will be discussed in detail in Chapter 5 "Notice-and-takedown procedure in the US, the EU and China".

174 Ibid, Sec. 512 (h). How the subpoena mechanism is applied in the US will be discussed in Chapter 6 "Disclosure of Internet users' identities in the US, EU and China".

175 Ibid. Sec. 512 (i).

176 Ibid. Sec. (m) (1).

177 German Teleservices Act (1997), Art. 5 (3), (4).

178 T. Kono, et al., *Selected Legal Issues of E-commerce* (Kluwer Law International. 2002), at 39.

The "safe harbor" for ISPs in the EU is provided in the Directive on Electronic Commerce, which means that the "safe harbor" provisions in the EU are not just limited to the area of copyright, but also include trademark and other areas relevant to electronic commerce.[179] Furthermore, the "safe harbor" provisions in the EU only cover three categories of ISPs, which is "mere conduit", "caching" and "host", but without dealing with liability in relation to information location tools such as hypertext links and search engines.[180] As for a notice-and-takedown procedure, because of worrying about its potential negative influence on the freedom of expression, the Directive did not adopt this procedure except making a general statement about it in the preface as following: "this Directive should constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information; such mechanisms could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States."[181] So the "notice-and-takedown" procedure in the EU mainly relies on each Member States' national laws.[182]

The first category of ISPs who can enjoy liability limitation is the ISP acting as a mere conduit. As for the elements of exempting liability, they are also similar to those provided in DMCA, as follows: "the ISP does not initiate the transmission and select the receiver of the transmission; does not select or modify the information contained in the transmission."[183] Besides, the storage of information transmitted should be solely for the purpose of carrying out the transmission within an automatic, intermediate and transient process, and the information transmitted cannot be stored longer than a reasonable period.[184]

The Directive also contains an exemption for ISPs, who make automatic, intermediate and temporary storage of information for the sole purpose of enhancing the efficiency of information transmission.[185] In order to comply with exempting conditions, the ISP cannot modify the information, must comply with conditions on access to the information and rules regarding the updating of information prevailing in that industry, and cannot interfere with the legal use of widely recognized and used technology by the industry to obtain data on the use of the information; and finally, the ISP should remove or disable access to the information expeditiously upon knowing the fact that the information at the initial source has been removed from the Internet, or by following the order from a court or an administrative authority.[186]

179 Peguera M, 'The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems' (2009) 32 Columbia Journal of Law & the Arts 481, at 483.

180 E-commerce Directive (n1), Art. 21.

181 Ibid, Recital 40.

182 In Chapter 5, the notice-and-takedown procedures in the EU Member States will be discussed in detail.

183 E-commerce Directive (n1), Art. 12.

184 Ibid, Art. 12.

185 Ibid, Art. 13.

186 Ibid.

The ISPs hosting a storage space for their users also enjoy liability exemption under the EU Directive, on the condition that: the hosting ISP "does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent;" and "upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the information."[187] The previously-mentioned liability exemption only applies when the recipient of the service is not acting under the authority or the control of the provider.[188] By comparing these elements above to that provided in US law, we can find that the elements like "control" and "direct benefits" from vicarious liability are not adopted by the EU Directive.[189] Because unlike in the US where the vicarious liability has already been developed as a common rule in tort law by case law, in the EU, the vicarious liability only applies when the direct infringer affiliates to the defendant, and it's too hard to prove that this kind of affiliating relationship exists between a hosting ISP and its users.[190]

The E-commerce Directive contains several general provisions that cover all three types of ISPs. First, Member States must not impose a general obligation on ISPs to monitor the information which they transmit or store, or a general obligation actively to seek facts or circumstances indicating illegal activity.[191] Second, the Member States may provide that, at the request of competent authorities, the ISPs should
50 forward the information enabling the identification of recipients of their service who commit alleged infringement to these authorities.[192] Third, the EU Directive indicates that injunctions can be ordered by courts or administrative authorities to require ISPs to terminate or prevent any infringement, such as removing illegal information and disabling access to it.[193]

2.2.3 Internet Regulation in China

When it came to the late of 1990s, with the prevalence of the Internet in China, more and more cases about copyright infringement on the Internet were appealed to the courts. For instance, in 1999, a hosting ISP was held liable for making two literary works publicly available on its platform upon a users' request but without the copyright owner's authorization.[194] Nevertheless, the legislators in China didn't

187 Ibid, Art. 14.

188 Ibid.

189 Peguera, 'The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems' (n175), at 491.

190 Wang Q and Guibault L, *Study on Online Copyright Regulation in China and Europe*, (Law Press 2008), at 83.

191 E-commerce Directive (n1), Art. 15.

192 Ibid.

193 E-commerce Directive (n1), Recital 45. The detailed discussion can be found in Section 4.3.2. "repeat infringement in the EU".

194 This case was heard by Haidian District Court (first instance) and Beijing 1st Intermediate People's Court (Second Instance), and both courts held the defendant liable. In 2000, this case was selected as a leading case by Supreme Peoples' Court. See Gazette of the Supreme People's Court No.1/2000 (最高人民法院公报2000年第1期), at 28.

prepare well for providing a new regulation about this complicated issue at that time, so in order to solve the problems which had already emerged, in 2000 the Supreme Peoples' Court in China promulgated a Judicial Interpretation relevant to resolving copyright disputes on the internet, particularly about ISPs' liability, which used the DMCA 512 as an important reference.[195] According to this Interpretation, the ISP which participates in, instigates, or assists in, copyright infringement by a third party, must take the infringing liability jointly with the third party;[196] the hosting ISP which actually knows its subscriber' infringement through its internet, or after receiving an evidential warning notice from copyright owners, but still doesn't take measures to eliminate infringement, will take responsibility for the infringement;[197] the hosting ISPs must offer the registration information of infringers to copyright owners, if the copyright owners ask for this information for launching suits against the infringers;[198] only the competent notice is valid, which should include the proof of the notifier's own identity, the proof of his copyright ownership and the proof of the infringement;[199] an ISP shall be exempted from the liability of breaching the contract, if it removes the alleged infringing content by following the competent notice; a copyright owner shall be responsible for the damage caused by his wrong notice.[200]

In the following years after promulgating the Internet Interpretation (2000), the development of the Internet went far beyond the expectation of the People's Supreme Court when providing this Interpretation, which means a lot of cases involving new technologies could not be regulated within the framework of this Judicial Interpretation. On the other side, the provisions in Internet Interpretation (2000) was so general that it left a lot of room for the lower courts to interpret in terms of their understanding, which resulted to major problems in judicial practice. Therefore, in order to solve the above-mentioned problems, in 2006, the State Council in China enacted the Regulation on the Protection of the Right to Internet Dissemination of Information (thereafter "Internet Regulation").

According to the Article 20, where any internet service provider provides the service of automatic access pursuant to the direction of its service recipients or provides the service of automatic transmission of works, performance and audio-visual products to its service recipients and if the following requirements are satisfied, it is not

195 Supreme People's Court (最高人民法院), Interpretation of the Supreme People's Court on Certain Issues Related to the Application of Law in the Trial of Cases Involving Computer Network Copyright Disputes (最高人民法院关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释) (thereafter Internet Interpretation (2000)), Fa Shi [2000] No. 48 (法释[2000]48号), November 22, 2000.

196 Ibid, Art. 4.

197 Ibid, Art. 5.

198 Ibid, Art. 6.

199 Ibid, Art. 7.

200 Ibid, Art. 8.

required to undertake the liabilities of compensation: [201] (1) having not chosen or altered the transmitted works, performance and audio-visual recordings; or (2) providing the works, performance and audio-visual recordings to the designated service recipients and preventing any person other than the designated service recipients from obtaining access. Compared to relevant provisions in DMCA and the EU directive, the Internet Regulation doesn't require that the information transmitted cannot be stored longer than a reasonable period.

As provided in Article 21, Where an Internet service provider obtains the relevant works, performance and audio-visual products from any other internet service provider for the purpose of elevating the efficiency of internet transmission to store the aforesaid works and provides them to the service recipients automatically according to the technical arrangement and in case the following requirements are satisfied, it is not required to undertake the liabilities of compensation: [202] (1) Having not altered any of the works, performance or audio-visual products that are automatically stored; (2) Having not affected the original internet service provider of the works, performance and audio-visual products in controlling the use of the relevant works, performance and audio-visual products; or (3) When the original internet service provider revises, deletes or shields the works, performance and audio-visual products, automatically revising, deleting or shielding according to the technical arrangement. By comparing to DMCA 512 and the EU Directive, the Internet Regulation does more favor to ISPs who run a caching system, because it doesn't require the ISPs to delete or remove the infringing contents in their system even after they know these contents are infringing the law.

52

The third "safe harbor" in Internet Regulation is provided to hosting ISPs, which is described in Article 22. Where an Internet service provider provides information memory space to its service recipients, for whom it transmits the works, performance and audio-visual products to the general public through the information internet and in the case where the following requirements are satisfied, he is not required to undertake the liabilities of compensation: [203] (1) clearly indicating that the information memory space is provided to the service recipients and publicizing the name, contact person and web address of the internet service provider; (2) having not altered the works, performance and audio-visual products that are provided to the service recipients; (3) having no knowledge of and no justifiable reason to be aware of the infringement of the works, performance and audio-visual products; (4) having not obtained any direct economic benefit from the works, performance and audio-visual products provided by its service recipients; and (5) after receiving a warning notice from the copyright owners, deleting those works, performance and

201 Internet Regulation (网络条例) (n1), Art. 20.
202 Ibid, Art. 21.
203 Ibid, Art. 22.

audio-visual products alleged as infringing ones by copyright owners according to this Internet Regulation.

Article 23 confers the last "safe harbor" to ISPs who run an information location service. [204] Where an Internet service provider offering any searching or linking service to its service recipients cuts off the link to any infringing work, performance, or audio-visual product after receiving a warning notice from the rights owner according to the provisions of Internet regulation, it is not required to undertake the liabilities of compensation. However, where anyone is actually aware of or should have known that any of the works, performance or audio-visual products it has linked to constitute any infringement, it shall be subject to the liabilities of joint infringement.

The Internet Regulation provides a detailed "notice-and-takedown" procedure, including the contents of the notice, the responsibility of ISPs, the contents of counter-notice, the liability of mistaken deletion, which refers a lot to DMCA 512. As provided in Article 14, the notice should at least include the following contents: (1) Name, contact information and address of the owner; (2) The names of the infringed works, performance and audio-visual products that are required to be deleted or the names of the web addresses whose link is required to be cut off; and (3) The preliminary evidential materials for proving infringement. After receiving a notice from the rights owner, the internet service provider should immediately delete the relevant works, performance and audio-visual products as suspected of infringement or cut off the link to the relevant works, performance and audio-visual products as suspected of infringement and should simultaneously transfer the notice to the service recipients that transmit the relevant works, performance and audio-visual products. Where the web address of a service recipient is not clear and therefore a transfer is impossible, the notice contents should be simultaneously announced on the information internet.[205] If the service recipient, who receives the notice concerning deletion from the ISP, deems that the deleted content does not infringe any other's copyright, it may file a written counter-notice to request restoring the deleted content, and the counter-notice should contain the following elements: (1) The name (title), contact method and address of the service object; (2) The names of the works, performance, audio-visual products as well as web addresses as requested for recovery; and (3) The preliminary evidential materials for proving non-infringement.[206] After receiving a written statement from a service recipient, the internet service provider should immediately recover the deleted works, performance and audio-visual products or recover the link to the works, performance and audio-visual products and should transfer the written statement

204 Ibid, Art. 23.
205 Ibid, Art. 15.
206 Ibid, Art. 16.

of the service recipient to the relevant copyright owner simultaneously, who cannot request the internet service provider to delete the works, performance and audio-visual products or to cut off the relevant link any longer.[207] Eventually, if the relevant ISP, as a result of the copyright owner's notice, wrongly deletes or cuts off the link to any work, performance or audio-visual product and therefore causes any loss to its service recipient, the copyright owner shall be subject to the liabilities of compensation.[208] From this Article, it can be inferred that the ISPs don't need to be responsible for wrong deletion by carrying out the copyright owners' notices.

The Chinese Internet Regulation also includes a provision about disclosing the identity information of alleged infringers. However, according to Article 13, the administrative department of copyrights may, with a view to investigating the infringements upon the right to internet dissemination of information, require the relevant internet service provider to provide such materials as the names, contact information, and the web addresses of its service recipients who are suspected of infringement. Furthermore, if any Internet service provider refuses or delays to provide such Internet materials as the name, contact information and web address of its service recipients as suspected of infringement, the administrative department of copyright must give it a warning. In the event of serious circumstances, equipment such as computers that are mainly applied to providing the Internet services will be confiscated.[209]

54

In addition, the Regulation lacks an important provision which clarifies that the ISPs should not be required to undertake a general obligation to monitor the information that they transmit or store, or a general obligation actively to seek facts or circumstances indicating illegal activity. Without the clear provision about general monitoring liability, the courts bear different opinions about this issue, which leads to confusion in judicial practice.[210]

Since 2012, the National Copyright Administration (China) has published three versions of an amending draft of Copyright Law, and all of them include an identical Article regulating the liability of ISPs. To begin with, this article makes a declaration about ISPs' general monitoring liability as following: when internet service providers provide storage, search, linking and other purely technological internet services to internet users, they do not bear a duty to monitor the information concerning copyright or related rights.[211] The following content of this article is similar as what provided in Tort Law. As provided in this article, where users use

207 Ibid, Art. 17.
208 Ibid, Art. 24.
209 Ibid, Art. 25.
210 It will be discussed in Chapter 4, Section 4.1.3.
211 National Copyright Office, Amending Draft of Copyright Law of the People's Republic of China (中华人民共和国著作权法修正草案), First Draft (March 2012), Art. 69; Second Draft (July 2012), Art. 69; Third Draft (June 2014), Art. 73. The amending draft is currently still pending.

the Internet to conduct copyright infringing activities or related rights, the injured person may notify the ISP in writing, and require it to adopt necessary measures such as deletion, shielding, breaking links, etc. Where the Internet service provider adopts the necessary measures in a timely manner after receipt of the notification, it does not bear liability for compensation; where it does not promptly adopt the necessary measures, it bears joint and several liability with the said Internet user. Where Internet service providers know or should know that Internet users use their Internet services to infringe copyright, and do not adopt necessary measures, they bear joint and several liability with the said Internet users.[212] Generally speaking, the Article in this amending draft makes no concrete change to the current framework of regulating ISPs' liability except for declaring that there is no requirement of general monitoring liability undertaken by ISPs.

Compared with the above-mentioned revision draft of copyright law which just provides some general and abstract rules about the ISPs' liability, the Judicial Interpretation issued by the Supreme People's Court tended to be more detailed and easier to enforce. After the promulgation of the Internet Regulation, the courts in China heard many relevant cases, but when applying the Internet Regulation, different courts had different interpretations of the same regulation, and sometimes two courts came to totally opposite decisions based on very similar case facts, all of which lead into a confusion between the ISPs and copyright-owning communities. Therefore, based on the research about both domestic and overseas cases, and consulting with relevant industrial beneficiaries and scholars, the Supreme People's Court issued "Provisions of the Supreme People's Court on Certain Issues Related to the Application of Law in the Trial of Civil Cases Involving Disputes over Infringement of the Right of Dissemination through Information Networks (thereafter Internet Provisions),"[213] which provides responses to the problems in judicial practice. The contents of Internet Provisions will be discussed in detail when Chinese case law is analyzed in the following chapters.

To sum up, after the first "safe harbor" provisions were adopted in the US, the EU and China also enacted their own "safe harbor" provision by referring to relevant rules in the US DMCA §512. By comparing the "safe harbor" provisions in the US, EU and China, one can find that the liability exemption is granted to different types of ISPs so as to ensure the ISPs' freedom to operate and promote the development of the Internet industry. With regard to hosting ISPs, many common points can be drawn from the "safe harbor"

212 Ibid.

213 Supreme People's Court, Provisions of the Supreme People's Court on Certain Issues Related to the Application of Law in the Trial of Civil Cases Involving Disputes over Infringement of the Right of Dissemination through Information Networks (最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定), Fa Shi [2012] No. 20 (法释〔2012〕20号) November 26, 2012.

provisions discussed above. First, hosting ISPs have no general obligation to monitor the materials uploaded on their platforms (in China it is still uncertain at legislative level). Second, in order to benefit from liability exemption, hosting ISPs should not know the infringement in question, or upon knowing the infringement, hosting ISPs should expeditiously remove the infringing materials. Third, in the light of the "safe harbor" provisions in the US and China, courts need to take into account whether hosting ISPs receive direct benefit from infringement when deciding whether to grant them liability exemption. Fourth, the US and EU require hosting ISPs to take certain measures against repeated infringement. Fifth, notice-and-takedown procedures have been codified in the US and China. Sixth, hosting ISPs need to fulfill certain obligations, such as disclosing suspected users' identities to copyright owners or competent authorities.

Table 1*

	No Monitoring Obligation	Knowledge	Direct Benefit	Repeated Infringement	NT Procedure	Identity Disclosure
US	√	√	√	√	√	√
EU	√	√	×	√	×	√
China	×	√	√	×	√	√

56 * *This Table describes a general comparison between "safe harbor" provisions in the US, EU and China. "√" means that the "safe harbor" provisions in this jurisdiction include the corresponding elements, and "×" means not. To be mentioned, even though two jurisdictions are both featured with "√" under one element, it does not mean these two jurisdictions have the same provisions on this element. Because of the limitation of this Table, the different provisions on one element in different jurisdictions cannot be demonstrated by this Table, and these differences will be exploited in the following chapters. In addition, even though a jurisdiction is featured with "×" under one element, as shall be seen in the following chapters, it does not mean the courts in this jurisdiction do not take into account this element when deciding upon a hosting ISPs' liability.*

2.3 Conclusion:

Regarding indirect copyright infringement, there is not so much harmonization at international level, so the rules about indirect copyright infringement are mainly rooted in national law, and the relevant rules in each nation are different from each other. In the US, the courts have developed contributory infringement and vicarious liability to deal with indirect copyright infringement. In the EU, except the UK where authorization infringement and joint tortfeasance have been developed to regulate indirect infringement issues in the copyright field, the other Member States, such as France, Germany and Italy, deal with indirect copyright infringement by referring to general tort law rules. In China, the courts also refer to liability rules in general tort law, when hearing cases about indirect copyright infringement. Nevertheless, in order to ensure the freedom to operate of hosting ISPs, a liability limitation rule called "safe harbor" provisions has been commonly adopted in the US, EU and China. Further,

the "safe harbor" provisions are not only related to deciding whether hosting ISPs need to be liable for copyright infringement on their platforms, but also bring in several mechanisms, in the light of which hosting ISPs need to fulfill certain obligations for the purpose of copyright enforcement on their platforms, so "safe harbor" provisions play an important role in regulating hosting ISPs' freedom to operate. In addition, although the "safe harbor" provisions in the US, EU and China have their own characteristics, they are homogenous per se and share many common norms. Therefore, in this respect, the norms on hosting ISPs' liability have reached a certain level of harmonization in the US, EU and China. However, as noted by Mousourakis, "law is more than simply a body of rules or institutions; it is also a social practice within a legal community" and "this social practice... shapes the actual meaning of the rules and institutions, their relative weight, and the way they are implemented and operate in society."[214] When interpreting "safe harbor" provisions, the courts in the US, EU and China will be unavoidably affected by the legal norms rooted in their traditions, especially the rules about indirect copyright infringement. Therefore, in order to preserve maximum freedom for hosting ISPs to operate in the US, EU and China, it is necessary to review how their responsibilities for copyright infringement are tailored by the courts under the roof of "safe harbor" provisions in these jurisdictions, which will be done in the following chapters.

214 Mousourakis G, 'Transplanting Legal Models across Culturally Diverse Societies: A Comparative Law Perspective' (2010) 57 Osaka University Law Review 87, at 90.

Chapter 3

Active or Passive: A Threshold for Hosting ISPs to Enter a "Safe Harbor"

Introduction:

Traditionally, courts held distributers and publishers strictly liable for any copyright infringement that appeared in their publications.[215] In others words, publishers are responsible for the copyright infringing content supplied by others but appearing in their publications. However, the hosting ISPs, who also distribute information supplied by others, are not held strictly liable for copyright infringing content that the ISPs distribute. The significant question is why the law treats similar acts differently depending on the source of distribution. The stated reason is the theoretical ability to control for potential copyright infringing acts.[216] A publisher, before it distributes any information originating from others to the public, needs to screen, select and edit it, which then makes the publisher responsible for the content that it distributes.[217] In essence, the editorial process of selection and organization makes the publisher the "author" of the infringing work.[218] By contrast, a qualified hosting ISP does not screen, select, or edit the information uploaded by Internet users, but only stores the information on its system at the direction of its users.[219] Many countries have adopted this policy into law. For example, the United States Senate Committee on the Judiciary adopted this concept of liability in its report, stating, "information that resides on the system or network operated by or for the service provider through its own act or decisions and not at the direction of a user does not fall within the liability limitation of subsection (c)."[220]

60 So, generally, the strict "liability is (only) ruled out for passive, automatic acts engaged in through a technological process initiated by another."[221] Similarly, the E-commerce Directive also states that the exemption from liability established in the Directive covers only cases "where the activity of the information society service provider is limited to the technical process of operating … activity is of a mere technical automatic and passive nature."[222] Further, in China, the hosting ISPs must not alter the works, performance and audio-visual products that are provided by the service recipients.[223] Therefore, in order to qualify for the liability limitation or safe harbor, the hosting ISPs should retain a passive and technical role during the transmission of content supplied by their users so as to avoid moving from being a passive conduit protected by the various safe harbor laws to being a publisher strictly liable for the content that it distributes.

215 Schuerman E, 'Internet Service Providers and Copyright Liability-Don't Touch... Or at Least Not Too Much: CoStar v. LoopNet' (2005), 30 Southern Illinois University Law Journal 573, at 575.

216 Spinello RA, *Regulating Cyberspace: The Policies and Technologies of Control* (Quorum Books. 2002), at 135-136.

217 Scruers M, ' The History and Economics of ISP Liability for Third Party Content' (2002) , 88 Virginia Law Review 205, at 233.

218 Ibid, at 245.

219 Bayer J, Liability of Internet Service Providers for Third Party Content (2008) 1 Victoria U. Wellington Working Paper Ser. 1, at 6-7.

220 Congress U.S., Senate Report, No. 105-190 (1998), at 43.

221 H.R. Rep. No. 105-551 (II) (n16), pt. 1, at 11.

222 E-commerce Directive (n1), recital 42.

223 Internet Regulation (网络条例) (n1), Art. 22.

However, the hosting service offered by ISPs has been significantly developed in the past decade. Before, the contents of hosting websites were almost completely created and organized by the Internet users. Nowadays, with the aim of reaching a better position in the market, hosting ISPs always take some measures to optimize their service, such as facilitating or restraining the creation of certain kinds of content, making Internet users access their desired content more easily by designing specific web frames, and generating profit by displaying ads with relevant content. [224] Can these developed hosting ISPs still conform to the definition of "a passive and technical role"? The relevant legislations drafted 10 years ago cannot give us a clear answer, so the more recent judicial decisions on this issue need to be analyzed. However, it seems that the courts in different jurisdictions (applying national laws and local canons of statutory construction) make different interpretations about "a passive and technical role", so it is necessary to compare the relevant cases in these different jurisdictions and then to analyze the relevant factors considered by the courts, and finally determine the decisive factors on which there needs to be a focus, so as to preserve maximum freedom for hosting ISPs to conduct business in the US, EU and China.

This chapter first explores how the courts in China interpret the "alteration" of uploads so as to disqualify the less passive hosting ISPs for "safe harbor" provisions (3.1). Then, it examines the factors on the basis of which the courts in the EU (France, Germany, Italy and the UK) consider hosting ISPs to be content providers like publishers (3.2). In the US, hosting ISPs' competence for "safe harbor" provisions has also been challenged before the courts, and this chapter (3.3) discusses the US case law ruling on what is a prescribed hosting ISP in the "safe harbor" provisions. Based on the comparison between China, the EU and US, it summarizes and evaluates the relevant factors considered by courts when deciding on the hosting ISPs' competence for "safe harbor" provisions (3.4). The factors evaluated in Section 3.4 can be seen as conducting a certain degree of management on the uploaded contents, so the next Section discusses whether a hosting ISP should be required to keep purely passive or allowed to conduct certain management, and then draw a criterion for deciding what is a qualified hosting ISP defined in "safe harbor" provisions (3.5). Finally, it summarizes and concludes the findings in the previous sections (3.6).

224 de Azevedo Cunha, M. V., Marin, L., & Sartor, G., 'Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web' (2012) 2 International Data Privacy Law 50, at 50-51.

3.1 China

Chinese law does not explicitly require hosting ISPs to maintain a passive role when transmitting the information, but this requirement can be deduced from Article 22 (2) requiring hosting ISPs not to alter the works, performance, or audio-visual products that are provided by the service recipients.[225] If the hosting ISPs actively alter contents uploaded by users, it means that they no longer play a passive role; and under certain circumstances, the altered contents will be seen legally as the ISPs' own content. Therefore, how to define the "alteration" becomes an important question before Chinese courts. In the following factual scenarios, Chinese courts have found that the hosting ISP had sufficiently altered the user-supplied-content to be held liable.

3.1.1 Displaying Hosting ISPs' Logo

In the case of *Hua Xia Shu Ren vs. Youku*, the defendant, Youku was a video-sharing website similar to Youtube, and the plaintiff, Hua Xia Shu Ren owned the copyright to the alleged infringed works. In this case, the plaintiff found some of its copyrighted works being illegally uploaded by a network user called "Qilingjiao" to the defendant's website Youku, and then sued Youku for copyright infringement. According to the evidence exhibited during the hearing, when a user clicked on the alleged infringing videos, before the videos started to play, the screen turned black
62 temporarily and showed the defendant's logo "youku.com". Furthermore, during the playing of videos, the defendant's logo always appeared at the upper right corner of videos. Based on these facts, the Haidian District Court in Beijing held that these logos did not exist in plaintiff's videos, and also the logos could not be added by the users when uploading the videos, so these logos must have been added either by the defendant itself, or automatically added by responding software when the users uploaded the videos. In either case the defendant altered the alleged infringing videos uploaded by users through the adding of its logos, which functioned as an original sign of these videos.[226] If one follows the logic of the court's conclusion, it seems that, by adding logos into the videos, the defendant treated the videos as its own content, or at least made users believe those videos were coming from the defendant.

3.1.2 Inserting the Advertisements

In the case of *joy.cn v. 6room.com*, the plaintiff joy.cn was a video portal site which bought licenses for internet transmission from the copyright owners and then made those videos accessible to the public on its website. This service was similar to that provided by Hulu. The defendant 6room.com was a video-sharing website

225 Ibid.

226 *Guang Dian Wei Ye* v. *youku.com (广电伟业 v. 优酷)*, Beijing Haidian District Court (北京海淀区法院), (2008) Hai Min Chu Zi No. 9200 (2008海民初字 9200).

for network users to upload videos, which streamed some videos, for which the plaintiff had exclusive licenses for Internet transmission. According to the facts recognized by the court, before and after the playing of alleged infringing videos, 6room.com displayed advertisements, and whenever a viewer clicked on the pause-button, an advertisement would also appear. Furthermore, it was impossible for Internet users to add these advertisements when uploading, so defendant must have pre-integrated the advertisements into flash-player. Therefore, the court concluded that 6room actually altered the alleged infringing videos supplied by Internet users when it added advertisements.[227]

3.1.3 Generating a Collection of Uploaded Content

In the case of *Guang Dian Wei Ye v. youku.com*, Internet users uploaded episodes from a TV series owned by the plaintiff Guang Dian Wei Ye onto the defendant's website without permission, so the plaintiff sued the defendant Youku for copyright infringement. During the hearing, the court found that the defendant's website contained three collections consisting of episodes from this TV series, which facilitated the viewing of the infringing episodes.[228] Although the defendant claimed that each of the three collections were automatically produced when users clicked over from one relevant video to another a sufficient number of times to draw the connection rather than any affirmative editing doing so, the court held that this argument was not convincing, because the clicking over in the second collection amounted to a mere 277 clicks which were far fewer than for a normal technical system to automatically create a collection. Therefore, the court concluded that these three collections were edited and integrated by the defendant itself. Above all, the court held that the defendant altered the videos uploaded by internet users.[229]

To sum up, the interpretation of hosting ISP alteration of user-supplied content by Chinese jurisdictions can be divided into three types: first, a loose standard, where adding anything into the uploaded contents may constitute alteration, such as pop-up ads; second, a more moderate standard, focusing on whether the viewers could believe the content was offered by the hosting ISP, an example of indicia which could be displaying logos when the contents are viewed, which may confuse the viewers about the origin of content; third, a strict standard, where the hosting ISPs need to edit and

227 *joy.cn v. 6room.com (激动网v.6房间)*, Beijing Haidian District Court (北京海淀区法院), (2008) Hai Min Chu Zi No. 22186 (2008海民初字9200).

228 Generally, the internet users need to upload the episodes one by one, so the uploaded episodes scatter through the network system without good order, and it is not convenient for viewers to watch these episodes in sequence, even with the help of a built-in searching engine offered by website. But the collection solves this problem, because it integrates the episodes of a TV series all together in sequence so that the viewers can easily find the episodes they would like to watch by visiting the collection.

229 *Guang Dian Wei Ye v. youku.com (广电伟业 v. 优酷)*, Beijing Haidian District Court (北京海淀区法院), (2008) Hai Min Chu Zi No. 14023 (2008海民初字 14023).

integrate the uploaded content, similar to work done by publishers. While the courts have in practice applied three different standards; according to Guiding Opinions published by the Beijing Higher Court, the first two standards are unreasonable.[230] Although this Guiding Opinions is not a mandatory legal document, it still has widespread influence in China.[231] As indicated in this Guiding Opinions, the following conduct should not be seen as altering the works, performances, or audio-visual products that are provided by service accepters: 1) simply altering the storage format of the works, performances, or audio-visual products; 2) simply adding digital watermarks, such as websites' logos, onto the works, performances, or audio-visual products; 3) displaying ads before or after the playing of the works, performances, or audio-visual products, or pop-up ads during the playing of the works, performances, or audio-visual products.[232] Furthermore, the Internet Provision (draft) published by the People's Supreme Court also includes a similar article which exempts hosting ISPs from liability under the circumstances of altering storage formats or adding digital watermarks, but leaves the displaying of ads open.[233] However, it must be mentioned that this article did not appear in the final version of the Internet Provision which came into force from the beginning of 2013.[234] It seems that the method of defining "alteration" provided in the Regulation still needs to be discussed further.

64 ## 3.2 European Union

As already mentioned above, the EU E-Commerce Directive specifically requires ISPs to maintain a passive role when transmitting information if they wish to avoid liability for copyright infringement. So in the EU, whether the hosting ISPs have kept to a passive role is always debated during hearings about hosting ISPs' liability. Before the ECJ provided some guidance about how to decide whether a hosting ISP oversteps the border of passivity in Adwords decision[235], the courts in member states have already made several decisions about this issue. This section first examines the relevant case law in several member states, and then explores how the case law in member states interacts with the ECJ Adwords decision.

230 Beijing High People's Court (北京市高级人民法院), Opinions of Beijing High Court on Several Issues Concerning Disputes about Internet Copyright Infringements (trial) (北京市高级人民法院关于网络著作权纠纷案件若干问题的指导意（试行）) (thereafter "Guiding Opinions (指导意见)"), JingGaoFaFa[2010] No. 166 (京高法发[2010] 166号), May 19, 2010.

231 Unlike People's Supreme Court in China, the Beijing High Court has no statutory rights to promulgate any judicial interpretation of general application. However, Beijing, as one of two cities (the other is Shanghai) covering most of the disputes about internet copyright infringements in China, always takes a lead in solving these disputes, and also has accumulated lots of judicial experience in this aspect. Therefore, the Guiding Opinions provided by the Beijing Higher Court definitely has widespread influence in China, and will be used as an important reference by other courts.

232 Guiding Opinions (指导意见) (n229), Art. 24.

233 Internet Provisions (n208) (draft) (网络条例(草案)), Art. 13.

234 See the Internet Provisions (网络条例) (n208).

235 Joined Cases C-236/08 to C-238/08, *Google France SARL and Google Inc. v Louis* Vuitton Malletier SA and Others, [2010] ECR I-02417. This case will be discussed in the end of this Section.

3.2.1 France

In the case of Tiscali, copyright owners Dargaud Lomlard and Lucky Comics, noticed in January 2002 that, without their permission, their two comic albums had been entirely reproduced and were available on defendant Tiscali's video-sharing website. So, they sued Tiscali. During the appeal, the judges of the Paris Court of Appeal concluded that Tiscali also acted as a publisher, since the services provided went beyond the mere technical features defined as hosting. The appellate court stated the following reasons to support its findings: First, "Tiscali Media offers its users the feature of creating their personal pages from its website, www.tiscali.fr, and that goes beyond a merely technical service." Second, "Tiscali Media has to be considered as a publisher as well (i.e. liable for the content), since it commercially exploits the website by offering advertising space directly on personal web pages, such as www.chez.com/bdz."[236] In the final instance, the First Civil Division of the French Supreme Court (also) considered these facts as sufficient to establish that the services provided by Tiscali went beyond the simple technical functions,[237] although the Supreme Court did not hold Tiscali Media' activities as those of a publisher.[238] In a similar case involving a video-sharing website called "MySpace," the French High Court of First Instance held that defendant MySpace was a publisher by following the same line of analysis, namely, "allowing members to create personal web pages within a specified frame structure, including video uploading; and that each time a video posted by a member is viewed, advertisements from which MySpace profits, are broadcast."[239]

However, what is more interesting is that the First Civil Division of the French Supreme Court, which dealt with the *Tiscali* case, reached the totally opposite conclusion in the factually similar *Dailymotion* case, which it decided shortly after *Tiscali*. According to the court in the *Dailymotion* case, the key point is whether a hosting ISP tries to influence the uploaded contents or is just optimizing its service, and the following conduct by the defendant was proper. First, technical operations done by the defendant *Dailymotion*, such as "re-encoding videos in order to make them compatible with the viewing interface, and formatting them in order to make optimal use of the server's storage capacity by limiting the size of uploaded files", was necessary for running a hosting platform and irrelevant to selection of uploaded content.[240] Second, Dailymotion's optimization of its hosting service, such as

236 *See* Matulionyte R and Nérisson S, 'The French Route to an ISP Safe Harbor, Compared to German and US Ways' (2011) 42 International Review of Industrial Property and Copyright Law 56, at 58.

237 Ibid, at 59.

238 Ibid.

239 Stephen W. Workman, Internet Law - Developments in ISP Liability in Europe, *available at* http://www.ibls.com/internet_law_news_portal_view.aspx?id=2126&s=latestnews [last visited July 26, 2013].

240 Amélie Blocman, Liability of Video-sharing Platforms - First Judgement of Court of Cassation, *available at* http://merlin.obs.coe.int/iris/2011/3/article18.en.html [last visited July 26, 2013].

"setting up of presentation frames and tools for classifying content," was reasonable, because these measures met with the need of users to set up their own individual web pages and more easily access their desired content; more importantly, these measures imposed no influence over the content uploaded by users.[241] Finally, using defendant's website for displaying ads was just a way to make profit, and would not influence the uploaded content.[242]

3.2.2 Italy

In Italy, after the Supreme Court introduced a concept of "active hosting" in a criminal case against the Pirate Bay, Civil Courts also started to decide hosting ISPs' liability by referring to the theory of active hosting.[243] According to relevant judicial interpretation, active hosting means that the hosting ISP which is somewhat active (or minimally active) still cannot be treated as a publisher from a legal perspective, even though its conduct goes beyond being a merely "passive" ISP within the meaning of Recital 42 of the E-Commerce Directive, which provides the hosting ISP liability exemption.[244] For instance, the District Court of Milan held IOL and Yahoo! as active hosting ISPs based on their following activities:

1) they provided for a system that allowed the publication of advertising links related
66 to the videos; 2) the user terms and conditions of the websites included a license agreement, according to which users grant IOL and Yahoo! inter alia the right to display, edit, adapt, modify and use the uploaded videos; 3) they provided a search engine service allowing the indexing of the uploaded videos and their contents, thus amplifying their visibility. This service also allowed the indexing of so-called related videos, ie videos which were related to those searched for by the person surfing the internet and using the service in question; 4) finally, IOL and Yahoo! uploaded some videos on their websites themselves.[245]

In another case, the District Court of Rome also held that YouTube was running an active hosting service, and the reasons were the following: 1) YouTube could properly control the uploaded contents, since the terms of service on its website indicated that YouTube had the right to remove any uploaded content, terminate users' accounts, and unilaterally change the terms; 2) the YouTube organized the infringing

241 Ibid.
242 Ibid.
243 Bellan A, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in Italy' in Heath C and Sanders AK eds., *Intellectual Property Liability of Consumers, Facilitators, and Intermediaries* (Kluwer Law International 2012), at 108.
244 Bonadio E and Santo M, 'Court of Milan holds video sharing platforms liable for copyright infringement' (2012) 7 Journal of Intellectual Property Law & Practice 14, at 15.
245 Ibid.

content so as to make more revenue from ads, because, on its website, an internal search box could be used for indexing and finding infringing content.[246] Based on similar criteria, the District Court of Rome concluded several other hosting ISPs to be actively hosting or staying neutral.[247]

3.2.3 Germany

In Germany, under certain circumstances, hosting ISPs are liable as content-providers for their own content (die Haftung als Content-Provider fuer eigene Inhalte), which means, if a hosting ISP plays a content-provider-role, it shall be responsible for the content uploaded by users as if the content was offered by the ISP itself. To determine under what circumstances a hosting ISP shall be deemed a content-provider, one must to refer to judicial decisions.

3.2.3.1 Photo Platform Pixum - OLG Hamburg

In this case, the defendant operated a photo platform, called Pixum, for the public to upload photos. Pixum then charged subscribers for each download of one of these photos. The plaintiff was a photographer who found that three of his copyrighted photos were downloadable from Pixum, so he sued for copyright infringement. The Oberlandesgericht des (Higher Regional Court of) Hamburg concluded that the defendant was a content provider rather than a hosting ISP, based on the following reasons: 1) the photos uploaded by users in the open-access album constituted the only substantial contents of the website; 2) each viewer of the website could put the chosen photos, which were in open-access albums, into their shopping carts, and then send them to their cell phones by clicking on the function-buttons of the website, by which it collected money from photos subscribers; 3) the invoices for this kind of service were under the signature of the defendant, and the uploading-users did not share the profits. Therefore, the court held that, from the view of reasonable users, these photos were offered by the website operator. Furthermore, unlike the unidentified pseudonym used by the actual photo providers, the name and logo of the defendant, which moved as a background, was big and clearly visible. According to the terms and conditions of service set by the defendant, the uploaders of photos were required to grant part of their rights to the defendant so that the defendant could make money by offering the photo service.[248] These two facts also persuaded the court to believe that these photos were offered by the website operator, from the view of reasonable users. If we look into this decision, we can find that the Higher Regional Court of Hamburg applied a standard called "from the view of reasonable users" so as to decide whether user generated content should be treated as the hosting ISPs' own content.

246 See Bellan, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in Italy' (n238), at 110-111.

247 Ibid.

248 See OLG Hamburg, ZUM 2009, 642, at 645 – Pixum.

3.2.3.2 Platform for Photos Exchange – KG Berlin

In this case, the defendant operated a platform for its users to exchange their photos, and the Plaintiff found his photos were publicly accessible on the defendant's platform without his permission, so he sued the defendant for infringement.[249] Based on the following reasons, the Appeal Court of Berlin concluded the defendant was a content provider: 1) the defendant received 40 percent of fees paid by the users who downloaded the photos, and the rest of fees were distributed to the users who offered these photos for sale; 2) the uploaded photos went through a selecting and checking procedure before they were publicly accessible; 3) the copyright owners of the photos were pointed out, but in an unnoticeable way; 4) in the front part of the website, the corresponding philosophy of the operator was displayed under its logo, which was "publish modern and time-spiritual photos." The above-mentioned facts would lead objective viewers to conclude that the operator of this platform was providing the public-accessible photos by itself.[250] Therefore, in the light of the understanding by the Appeal Court of Berlin, making profits, editing uploaded content, and the overall design of a website may attribute content to a hosting ISP. What is meant by an objective viewer? Inferring from judicial decisions, it has the same substantial meaning as "reasonable user."

3.2.3.3 YouTube – LG Hamburg

68 In this case, the plaintiff found a music work which he owned, publicly accessible on YouTube, so he sued YouTube for copyright infringement. Landesgericht des (Regional Court of) Hamburg concluded that YouTube was a content provider because: 1) the logo of YouTube appeared on the upper right corner of videos, due to a pre-designed website frame, but, in contrast, the pseudonym of the uploading users is very small and appears on a separate part of the website from the videos; 2) the defendant sorts the uploaded videos into different categories,[251] and when a video is clicked, similar videos will show up on the right side of the webpage automatically; 3) YouTube commercially exploits the uploaded videos by selling ad space, and requires the uploaders to grant it the right to use these videos.[252] As for commercial exploitation, the court further stated that only the commercial exploitation of the third parties' content cannot transform an internet hosting platform to the content provider, but the active integration of third parties' content

249 Actually, it's a case about portrait right rather than copyright, because the plaintiff is the person who was photographed in the picture but not the person who photographed the picture. However, the court in this case made a very detailed analysis about under what circumstances a hosting ISP shall be seen as content provider, so it deserves to be discussed.

250 See KG: Internetplattform zum Austausch von Fotodateien, 2010 MMR 203, at 204.

251 YouTube argued that it did not sort the uploaded videos into different categories, but it was the uploaders who decided which category they would upload the videos to, using the uploading conduit. However, the court rejected this argument, because it believed that, as objective viewers, they did not know about the above-said categorizing process.

252 *See* LG Hamburg: Haftung eines Plattformbetreibers – YouTube, 2010 MMR 833, at 834.

into the host platform's own commercial offers can result in liability.[253]

3.2.3.4 Chefkoch.de - BGH

In this case, the defendant operated a website called chefkoch.de, which allowed the public to upload cooking recipes and corresponding photos. The plaintiff ran a website called marions-kochbuch.de, which introduced cooking recipes with depicting pictures. The plaintiff found that some of his copyrighted cooking introductions had been uploaded to the defendant's website, so he launched a suit against the defendant for copyright infringement. By comprehensive consideration of overall relevant facts, the Bundesgerichtshof (Federal Court of Justice) concluded that the defendant was a content provider. First, in the light of existing evidence, the recipes were activated only after they had been edited, such as carefully selecting, checking the accuracy and completeness of the recipes, making sure that the characters of the recipes conformed to the standards of professional products, and then, through activation, the edited recipes were displayed on the website www.chefkoch.de. Second, the recipes and corresponding photos were presented under the defendant's logo, which was a cooking hat; furthermore, under the mode of print preview, the recipe also displayed under the defendant's logo, which was much bigger than the concealed uploader's alias.[254] Third, the uploaders of recipes needed to agree that the uploaded contents, including recipes, photos, and text, could be copied or transmitted in other ways by the defendant itself and third parties. Fourth, the defendant exploited the recipes commercially. To summarize, from the view of an objective user, the defendant did not keep a serious and sufficient distance from the uploaded content, so it could not benefit from the liability limitation enjoyed by pure internet-access, caching, and hosting ISPs as provided in the EU E-Commerce Directive.[255]

69

To sum up, in Germany, the courts conclude whether the hosting ISP crosses the borderline as a passive ISP defined in the Directive, by following a standard called "from the view of objective users," which means, if an objective user believes or has reason to believe the content on the platform is provided by hosting ISPs, then the hosting ISPs shall be treated as content providers and be subject to strict liability. Generally speaking, when applying this standard, the court will comprehensively consider whether the defendant has taken the following steps: implementing preliminary editorial control, integrating the uploaded content as the substantial editorial content of the website, inserting the website's logo or digital water print

253 Ibid.

254 According to the court's opinion, normally the users needed to print out the recipes so as to read them in the kitchen, so the printing form of recipe was an important factor to consider when judging whether an objective viewer would believe the recipe was offered by the defendant.

255 BGH: Verwendung fremder Fotografien für Rezeptsammlung im Internet – marions-kochbuch.de, 2010 NJW-RR 1276, at 1276-1278.

into third party's content, transferring the using rights of uploaded content through "terms and conditions," and commercially exploiting uploaded content by website operators.[256]

3.2.4 UK

In the UK, the courts also examined whether hosting ISPs should be held as publisher from legal perspective in several cases. In the case of *Tamiz v. Google*, Google ran a platform "Blogger" which allowed Internet users to create their independent blogs, and the plaintiff Tamiz found that one blog hosted on Blogger published several articles which were defamatory of him, so he sent notices to Blogger and requested the takedown of the articles in question.[257] After more than one month, the defamatory articles were voluntarily removed by the blogger, so Tamiz claimed that after being notified, Google became a publisher who could control the defamatory articles and hence was liable.[258] After examining the business model of Blogger, the Court of Appeal held that Google was not a publisher based on following reason. First, since 25000 new words was added to Blogger every minute, it was virtually impossible for Google to exercise editorial control over the contents hosted on Blogger.[259] Second, being notified could not convert Google's status or role into that of a publisher.[260] Third, being capable of taking down articles on Blogger was
70 irrelevant to conclude whether Google had been a publisher.[261] Besides, in this case, Google displayed advertisements on blogs hosted by it, and shared the advertising revenues with bloggers.[262] But the court did not take it into account when deciding on Google's legal status. Therefore, whether making profits is not a factor to hold hosting ISPs as publishers in the UK.

Further, whether a defendant is a competent hosting ISP or a publisher relies on whether the defendant controls or edits the content in question, and the hosting ISP's controlling or editing of other contents is irrelevant. In the case of *Kaschke v Gray and Hilton*, Mr. Gray posted the blog alleged to be defamatory to Ms. Kaschke on the website which was controlled and operated by Mr. Hilton, so Ms. Kaschke sued both Mr. Gray and Mr. Hilton for infringement.[263] According to the verified

256 Klein, CJ, *Haftung von Social-Sharing-Plattformen: Diensteanbieter zwischen Content-und Host-Providing* (Beck. 2012), at 72.

257 *Tamiz v Google Inc.*, [2013] EWCA Civ 68, para. 1. Although this is a case about hosting ISPs' liability for defamation, since the defamation issue is also covered by Article 19 of Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013), this case is still a good example to inspect how the UK differentiates between publishers and hosting ISPs.

258 Ibid, para. 2.

259 Ibid, para. 16.

260 Ibid.

261 Ibid.

262 Ibid, para. 1.

263 *Kaschke v Gray and Hilton*, Queen's Bench Division, [2010] EWHC 690 (QB).

> facts, Mr. Hilton had exercised some editorial control on parts of website, especially the homepage, which went beyond the mere storage of information at the direction of Internet users.[264] However, the court still held Mr. Hilton as a hosting ISP entitled to liability exemption, because it is irrelevant that the defendant had done editorial control on his website as a whole or its homepages or even the general storage of blog posts on his website, and in this case the real point was whether Mr. Hilton had done editorial control on the post which was the subject of the complaint from the plaintiff.[265]

In the EU, apart from the UK courts, the courts in France, Italy and Germany tend to hold hosting ISPs as publishers or entities similar to publishers from a legal perspective based on the following reasons, such as displaying advertisement, displaying logos, requesting the transfer of rights, setting different categories for uploading, editing the contents uploaded by users, etc. and then deprive hosting ISPs of "safe harbor" provisions. In the Google *Adwords* case, the ECJ discussed how to decide whether a defendant is still a competent hosting ISP protected by "safe harbor" provisions, and stated that, "it is necessary to examine whether the role played by that service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores."[266] Thus, the ECJ clarified that merely setting the payment terms or providing general information to its clients cannot have the effect of depriving Google of the exemptions from liability provided for in Directive 2000/31.[267] Therefore, by following this line of judicial analysis, in determining whether an ISP plays a passive role, it is irrelevant whether it receives profits by selling ad space, and so is the displaying of logos and allowing users to set up their own individual web pages. With regard to requesting the transfer of rights, setting different categories for uploading, editing the contents uploaded by users, it needs to examine whether these measures leads to a hosting ISP's knowledge or control of uploaded contents according to the facts in individual case.

3.3 United States

As the first country which officially provided a "safe harbor" provision to limit ISPs' liability, the United States courts also seem to interpret US law to broadly protect hosting ISPs from liability. So far, no hosting ISP has yet been treated as a content provider, even in a case where the defendant set a previewing procedure before allowing the user-uploaded photos to be displayed on its platform. In this case, the defendant, called LoopNet,

264 Ibid, Para. 77-80.
265 Ibid, Para. 89.
266 *Google France SARL and Google Inc. v Louis Vuitton Malletier SA and Others* (n230), para. 114.
267 Ibid, para. 116.

operated a web hosting service that enabled users to post commercial real estate listings. According to "terms and conditions," if a listing included a photograph, the user had to agree not to post copies of the photograph without authorization, and warrant that he or she had all necessary rights and authorizations from the copyright owner of the photograph. More importantly, a LoopNet employee would preview the photograph (1) to determine whether the photograph in fact depicted commercial real estate, and (2) to identify any obvious evidence, such as text message or copyright notice, that the photograph may have been copyrighted by another. If the photograph failed either one of these criteria, the employee deleted the photograph; otherwise, the employee would click the "accept" button.[268] This previewing procedure implemented by employees is a typical editing procedure undergone by publishers before publishing any content, so as to ensure that the published content conforms to their needs. According to the relevant decisions in the EU, LoopNet would certainly be treated as a content provider. However, the United States Court of Appeals for the Fourth Circuit held that LoopNet still qualified as a passive hosting ISP for the following reasons: 1) this previewing procedure for each photo took only seconds, which did not amount to "copying", nor did it increase LoopNet's volition in storing the copy; 2) the employee's look was so cursory as to be insignificant, and if it had any significance, it tended only to lessen the possibility that LoopNet's automatic electronic responses would inadvertently
72 enable others to trespass on a copyright owner's rights.[269] Therefore, in the light of the Fourth Circuit's opinion, the preview procedure was too short to make the uploaded photographs its own, and this procedure would only reduce the infringements, but not increase the infringements, both of which confirmed that LoopNet still qualified as a hosting ISP.

Actually, the *LoopNet* decision further lowered the threshold for avoiding direct liability formulated by the *Netcom* decision, which has been seen as one of the most important judicial references for the US legislators when they drafted DMCA 512.[270] According to *Netcom*, Netcom did not take any affirmative action that directly resulted in copying the plaintiffs' works other than by installing and maintaining a system whereby software automatically forwarded messages received from subscribers onto the Usenet, and temporarily stored copies on its system,[271] which helped Netcom avoid undertaking direct infringement. So, generally, in order to enjoy liability exemption, no human intervention should be involved, which was not the case for LoopNet. Therefore, some scholars summarized these two cases as follows: Netcom instructed service providers to not touch; Costar (the plaintiff in LoopNet case) instructs them to touch, but only

268 See *CoStar v. LoopNet*, 373 F.3d 544, at 547 (4th Cir. 2004).
269 Ibid, at 556.
270 Patry WF, *Patry on Copyright* (Thomson/West. 2009), § 21:85.
271 *Religious Technology Center v. Netcom On-line Communications Services, Inc.* (n4), at 1368.

if it is not too much.[272] In addition, the "not too much" standard has been further developed by other cases that apply the DMCA 512. For example, in case of *Perfect 10, Inc. v. CCBill, LLC and CWIE, LLC*, the defendant CWIE was a web hosting company, and the plaintiff, Perfect 10, was a company who owned copyrights for a lot of porn photos. After finding some of its photos posted on websites hosted by CWIE, Perfect 10 sued CWIE for copyright infringement. the United States District Court, C.D. California held that, merely because CWIE reviewed its sites to look for blatantly illegal and criminal conduct, that was not sufficient to close the safe harbor to CWIE; such a reading of the statute would not be in line with purpose of the DMCA to encourage internet service providers to work with copyright owners to locate and stop infringing conduct.[273] Therefore, according to this case law, the preview can be done for legal purposes, such as getting rid of illegal content.

With the development of Internet technologies, hosting ISPs have adopted multiple new functions on their platforms so as to attract more users. However, copyright owners may cite these new functions as the evidence to challenge hosting ISPs' competence of being sheltered under the "safe harbor". Generally, if the new functions run automatically, the US courts will conclude that the new functions do not negatively affect defendants' competence as hosting ISPs. First, "transcodes" is irrelevant to the competence of defendants. In the case of *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, when a video was uploaded to the defendant's video-sharing websites Veoh, it would be automatically broken down into smaller 256-kilobyte "chunks" so as to make the video accessible to the public.[274] Besides, in order to make the video viewable on users' computers and other portable devices, Veoh's software automatically converted the video into Flash 7, Flash 8 and MPEG-4 formats.[275] The court held that such automatic "transcodes" performed "for the purpose of facilitating access to user-stored material," so Veoh was still a competent hosting ISP. Second, "playback" is irrelevant to the competence of defendants. In the case of *Viacom International, INC. v. YouTube, INC.*, the defendant YouTube offered users a "playback" function which would automatically "deliver copies of YouTube videos to a user's browser cache" in response to a user request, and the court held that this function would not cost YouTube's safe harbor.[276] Third, "related videos" function is irrelevant to the competence of defendants. In the case of *Viacom International, INC. v. YouTube, INC.*, the defendant YouTube ran a "related videos" function which could "identify and display 'thumbnails' of clips that are 'related' to the video selected by the user" based on the so-called computer

272 *See* Schuerman E, 'Internet Service Providers and Copyright Liability-Don't Touch... Or at Least Not Too Much: CoStar v. LoopNet', at 593.

273 *Perfect 10, Inc. v. CCBill, LLC*, 340 F.Supp.2d 1077, at 1105 (C.D. Cal. 2004).

274 *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022, at 1027 (9th Cir.2011).

275 Ibid.

276 *Viacom International, INC. v. YouTube, INC.* (n7)

algorithm, and the plaintiff claimed that this function constituted "content promotion" rather than facilitate accessing to stored content, and therefore fell out of the boundary of safe harbor.[277] However, the court concluded that the "related video" function was still protected by safe harbor based on the following two reasons: 1) it "is fully automated and operates solely in response to user input without the active involvement of YouTube employees;" 2) it "serves to help YouTube users locate and gain access to material stored at the direction of other users," which substantially functions as an access facilitator.[278] In fact, the definition of ISP provided in DMCA 512(k)(1) offers a base for the US court to define a competent hosting ISP in a broader sense. DMCA 512(k)(1) reads as follows:

> (A) As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.
>
> (B) As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefore, and includes an entity described in subparagraph (A).

74

The definition of ISPs in sub-paragraph (A) only applies to Internet access providers which are regulated in subsection (a), so the requirements, such as "between or among points specified by a user", "of material of the user's choosing" and "without modification to the content," are only applicable to Internet access providers.[279] The hosting ISPs are covered by the definition in sub-paragraph (B), which does not render any specific requirement, especially in the absence of any restriction on modifying user-uploaded contents, so a competent hosting ISP should not be limited to a mere storage locker.[280]

3.4 Analysis on the Factors Involved in Deciding Hosting ISPs' "Passivity"

According to the judicial decisions discussed above, one can find in the US and UK, the courts set a low threshold for hosting ISPs to fall under "safe harbor" provisions, but the courts in China, France, Italy and Germany tend to deny hosting ISPs' competency for "safe harbor" provisions for their lower level of passivity when providing services. After comparing the case law in China, France, Italy and Germany, it can be found that the courts in these jurisdictions do share some common reasons when concluding that

277 Ibid, at 39.
278 Ibid, at 40.
279 Ibid, at 39.
280 *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F.Supp.2d 1081, at 1088 (C.D.Cal.2008).

a defendant is not qualified as a hosting ISP, such as commercially exploiting the user generated content, editing or categorizing the uploaded content, displaying its logo with uploaded contents, or requiring rights transfers by "terms and conditions." Actually, just as stated at the beginning of this chapter, if one looks into the current business models adopted by the hosting ISPs, most of them will conform to at least one or two of these factors, which means they may not enjoy "safe harbor" anymore and be exposed to higher legal risk. In the following section, these factors will be evaluated to see whether they are proper reasons to shut hosting ISPs out of "safe harbor" provisions, and how to interpret these factors so as to preserve maximum freedom for hosting ISPs to operate.

3.4.1 Commercial Exploitation of Uploaded Content

According to the judicial decisions in the EU member states, if a hosting ISP is treated as a content provider, the court always refers to its commercial exploitation of uploaded content. However, the EU Commercial Directive does not set commercial exploitation as a factor to shut hosting ISPs out of the "safe harbor," and, actually, the legality of commercial exploitation has already been implied by the Directive, because, as a hosting ISP, it does not offer the content by itself, but just stores user-uploaded content without charging fees.[281] In order to make profits, of course, it needs to commercially exploit the uploaded contents.[282] As noted by the ECJ in Adwords Decision, merely setting the payment terms or providing general information to its clients cannot have the effect of depriving Google of the exemptions from liability provided for in Directive 2000/31.[283] However, "it is necessary to examine whether the role played by that service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores."[284] Therefore, when judging whether a hosting ISP is still qualified for the "safe harbor" provisions, the point is not whether it commercially exploits the uploaded content, but whether its way of commercial exploitation goes against a passive technical ISP. By following this logic, one can divide commercial exploitation into two types, which are "active" and "passive" respectively, depending on whether the hosting ISPs take the initiative to combine their commercial exploitation with concrete and specific contents. For example, if a hosting ISP has already known a specific content existed in its system, and then inserts ads into this content according to the character of this content, we can conclude that it is an active exploitation, which will place the hosting ISP outside of the "safe harbor". In contrast, if a hosting ISP inserts ads without caring about which content these ads would be displayed with, it

281 Nérisson, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in France' (n103), at 79.

282 Ibid, at. 79.

283 *Google France SARL and Google Inc. v Louis Vuitton Malletier SA and Others* (n230), at para. 116.

284 Ibid, at para. 114.

is a passive exploitation. For example, the hosting ISPs may insert ads according to a time schedule, which means in certain time brackets, certain ads will be displayed, no matter what content is viewed by subscribers.

The distinguishing between "active" and "passive" exploitation prohibits hosting ISPs from deliberately using infringing materials for profits, while preserving sufficient freedom for them to make profits through their services. Based on this distinguishing factor, targeted advertising, which is a widely-used way for internet companies to allocate ad space, can be deemed legitimate. The operation of targeted advertising is based on tracing internet users' surfing demographics.[285] For example, if an internet company finds out that an internet user always views web pages about cell phones, then, when this internet user logs on to the website operated by this company, ads about cell phones will appear. Therefore, it is a good way to make the ads reach potential consumers more accurately. According to the distinguishing point made above, targeted advertising can be grouped into "passive" exploration, because where the adverts are displayed depends on the automatic assessment of Internet users' recent viewing demographics rather than on the hosting ISPs' intentional choices. Therefore, targeted advertising should be allowed and cannot become a reason to shut the hosting ISPs out of the "safe harbor."

76 ### 3.4.2 Editing of Uploaded Content

The publishers, such as newspapers and journals, which traditionally exert editorial control over content, are generally responsible for the content they publish, because the presence of an editorial relationship indicates that traditional publisher liability should apply.[286] This duty arises from the fact that the publisher has an opportunity to know the nature of the content.[287] The editing is a preparation process before publishing, generally including selecting, revising, and arranging the materials to be published. So, through editing, the publishers have enough opportunities to know the nature of the content, such as whether the content is infringing. More importantly, the editing is also a process for a publisher to ensure that the published content reflects its goals and needs. In other words, through editing, the publishers treat the content originated from others as their own content. So definitely, the publishers should undertake responsibility for the content published by them.

What is worthy of note is that the aforementioned editing is a human-intervention process finished by editors, but not an automatic process enforced by technical installation, because only human editing can ensure that the published content reflects the publishers' will and make the publisher know the nature of content. Therefore, when coming to the liability of hosting ISPs, it is necessary for us to

285 Hoyle, M. D, U.S. Patent No. 6,141,010; Washington, DC (2000), U.S. Patent and Trademark Office..

286 Scruers M, 'The History and Economics of ISP Liability for Third Party Content' (n212), at 233.

287 Ibid, at 245.

distinguish between human editing and automatic editing. If a hosting ISP just edits or categorizes the uploaded content through the previously installed technical programs, but without enough human intervention, the hosting ISP cannot be treated as a publisher. Just like the common sense approach reached in Germany, filtering (checking the uploaded contents through technical measures) should not be seen to fulfill the knowledge in the sense of TMG § 10,[288] because the machine cannot replace the human to check whether the information is infringing or not.[289] Besides, for human editing, the hosting ISPs should prove that the editing prevents infringements rather than tolerates them, and even with this kind of editing, the hosting ISPs still cannot know the infringing nature of content. Otherwise, they are not qualified hosting ISPs. Actually, both copyright owners and hosting ISPs recognize that it is necessary to "edit" the users' uploads to a certain degree so as to prevent infringing materials from being uploaded. For example, according to the UGC Principles, hosting ISPs need to adopt content identification technologies to filter out infringing uploads, and hosting ISPs are encouraged to manually review all of the user-uploaded content as a complement or replacement to content identification technology, so long as the manual review is as effective as the identification technology in terms of eliminating infringing content.[290]

Distinguishing between technical editing and human editing allows hosting ISPs to adopt the latest technologies to optimize their services, since the editing that is done automatically through pre-installed technical programs will not shut hosting ISPs out of "safe harbor". Further, human editing should be restricted rather than absolutely prohibited, and hosting ISPs are allowed to conduct human editing which either contributes to reducing infringement on their platforms or does not result in their knowledge of the infringement in question.

3.4.3 Displaying Logos with Uploaded Contents

The websites' logos, at least to some extent, function as trademarks. Actually most of them have already been registered as trademarks. In the light of a trademark's functionality of distinguishing the origins of products or services offered by different entities, it does make sense to conclude that a hosting ISP treats the uploaded content as its own if it displays its logo with uploaded content. Furthermore, the viewers may deem the uploaded content to be offered by the hosting ISP because of its logo appearing with uploaded content. However, this argument is not as tenable

288 It is a provision about exempting hosting ISPs from liability in Germany, which is directly translated from Art. 14 of E-commerce Directive.

289 *See* Spindler G, et al., *Recht der Elektronischen Medien: Kommentar* (C.H. Beck. 2008), at 1530-1532. *See* also Fitzner J, Von Digital-Rights-Management zu Content Identification: *Neue Ansätze zum Schutz Urheberrechtlich Geschützter Multimediawerke im Internet: Eine Technische, ökonomische und Rechtliche Analyse* (Nomos. Baden-Baden 2011), at 289-290.

290 Principles for User Generated Content Services (n42), Art. 3.

as it appears. First, it is the hosting ISP's right to display its logo on its website so as to distinguish it from other websites, and as a website mainly consisting of content uploaded by users, it is unavoidable for the ISP to display its logo with uploaded content. Second, displaying logos works more like a way to differentiate its service rather than indicate the origin of content, because normally the uploaders' names would be attached with the content, although in an anonymous way. More importantly, displaying logos with uploaded content is a pre-installed technical process, which is irrelevant to any editing of uploaded content, and has no chance of resulting in a hosting ISP's knowledge of content. Therefore, displaying logos with content cannot work as a reason to treat hosting ISPs as content providers.

3.4.4 Requiring of Right Transfer

Normally, the "terms and conditions" provided by hosting ISPs will require the uploaders to transfer or at least renounce certain rights so as to ensure the further dissemination of uploaded content. As publishers, they always ask the authors to sign a contract to transfer distributing rights to them. Hence, in this aspect, hosting ISPs are similar to publishers, and maybe it is why so many courts took it as a reason to treat hosting ISPs as publishers. However, just as mentioned before, a publisher needs to accept strict liability mainly because of its editing of content, which gives it
78 enough opportunity to know the nature of the content. In the case of hosting ISPs, this kind of licensing process happens automatically once the users agree to upload any content, without involving any kind of editing or knowledge over the content, which means the hosting ISP still maintains a passive and technical role, and still can enjoy the shield of the "safe harbor."

3.4.5 Uploading Contents by Itself

Nowadays, on the one hand, in order to reduce the danger of being sued, and on the other hand, in the light of the need of commercial operations, more and more hosting ISPs start to cooperate with copyright owners, and try to get the licenses of some valuable content. For the licensed content uploaded by hosting ISPs themselves, it seems that the hosting ISPs are not passive or purely technical anymore. So the Italian court named the defendant IOL and Yahoo! as active hosting ISPs based on the facts that they uploaded some content by themselves.[291] Technically speaking, in these circumstances, the legal status of hosting ISPs is mixed with content providers and service providers, which goes far beyond the anticipation of legislators when they ratified the "safe harbor" provisions. Actually, it is quite common for legislation to lag behind the development of technologies, especially in the field of copyright. When the courts face such problems, they cannot simply interpret the legislation literally, but

291 *See* Bonadio & Santo, 'Court of Milan holds video sharing platforms liable for copyright infringement' (n239), at 15.

must always refer to the legislative purpose, so as to ensure a reasonable interpretation. As illuminated by the House Report of DMCA, "safe harbor" provisions preserve strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment.[292]

If we look into the practical effects resulting from this kind of cooperation between hosting ISPs and copyright owners, we can find that it is good for reducing the infringements, or at least the harm which accompanies infringements. The reason is, if a user, without permission, uploads copyrighted content which has already been licensed to the hosting ISP, from the perspective of the copyright owner, it is not a really harmful infringement anymore. Therefore, hosting ISPs' uploading of licensed content by themselves conforms to the legislative purpose of "safe harbor" provisions, and these hosting ISPs can still enjoy the liability exemptions. Besides, from the perspective of copyright owners, they are also willing to license their copyrighted works to hosting ISPs. For example, since 2006, YouTube has signed a series of agreements which involved a large amount of copyright licenses with several copyright giants.[293] Further, Youku, always referred to as Chinese YouTube, signed a 5-year licensing agreement with Sony Pictures Entertainment in 2012, and according to this agreement, Youku can offer more than 300 movies from Sony on its website for the public to view.[294] In addition, since merging with Toudou, Youku has got copyright licenses from Warner Brother, Dreamworks, Paramount, 21st Century Fox, Disney, and other copyright owners.[295]

It would be quite absurd to consider these hosting ISPs liable for they get licenses from copyright owners. Just as stated by the EU Advocate General Niilo Jääskinen, the same exemption should apply if "one or more of the exempted activities are combined with an internet content provider's activities."[296]

3.5 How to Define "Passivity" in Post Web 2.0

The previous section evaluates the factors that the courts rely on to deprive hosting ISPs of "safe harbor" provisions, and then concludes that most of factors are not rational anymore. As referred to in the beginning of this chapter, hosting ISPs should keep passive so as to fall into "safe harbor" provisions, and the factors evaluated above can be seen as certain management on uploads done by hosting ISPs, so it is understandable

292 H.R. REP. 105-551(II) (n16), at 49.

293 See Warner Music Group and YouTube Announce Landmark Video Distribution and Revenue Partnership (n30); CBS and Youtube Strike Strategic Content And Advertising Partnership (n30); Universal Music Group and Youtube Forge Strategic Partnership (n30); Sony BMG Music Entertainment Signs Content License Agreement with YouTube (n30).

294 YoukuTudou signed a 5-year copyright licensing contract with Sony Picture (优酷土豆与索尼音像签订五年版权协议) (n30).

295 Ibid.

296 Opinion of Advocate General, *L'Oréal SA and Others v eBay International AG and Others*, case C-324/09, at para. 148.

that the courts deprive them of "safe harbor" provisions based on these factors. However, keeping passive does not mean being purely passive, and the following section will demonstrate why keeping passive is out of date and hosting ISPs should be allowed to conduct certain management of uploads.

First, one should take the development of new internet technologies into account. In the post web 2.0 era, the new technologies to some extent make management of hosted contents available, by which hosting ISPs can offer a better service, such as allowing Internet users to individualize their web pages, and facilitating access to desired content by various indexes; and hosting ISPs can also make better profits mainly through selling ad space. This management not only allows the public to express themselves better and promotes the public's access to information, but also benefits the development of e-commerce. The former conforms to the basic human right of "freedom of expression"; the latter meets with the policy objective of the "safe harbor" provisions.[297]

Furthermore, the recent case decisions show us a tendency that the courts in the EU, US, and China have started to require or at least encourage hosting ISPs to take certain monitoring measures for the uploaded content, which actually forces hosting ISPs to keep from being purely "passive." For instance, in China, the new Judicial Interpretation issued by People's Supreme Court provides that, if an ISP can prove that reasonable and effective technical measures have been taken, but the infringement committed by
80 Internet users still cannot be detected, People's Courts should conclude the ISP bears no fault for the infringement.[298] In a classic case named as *HanHan v. Baidu*, before the hearing, the defendant Baidu asked its employees to manually check the uploaded content to filter out infringing content, and the Haidian District Court in Beijing didn't hold it as a reason to treat the defendant as a content provider.[299] In the US, Veoh, a video-sharing website has adopted some measures which essentially "enabled Veoh to terminate access to any other identical files and prevent additional identical files from ever being uploaded by any user," and the court defined these measures as "appropriate steps to deal with copyright infringements."[300] In Germany, Rapidshare, a hosting ISP, was required by German Federal Court of Justice to take comprehensive and regular control

297 As stated by the Committee on Commerce in H.R. REP. 105-551(II), "promoting the continued growth and development of electronic commerce" is one of two priorities of DMCA 512. In EU E-commerce Directive, the Recital (2) emphasizes the significance of e-commerce for the EU, and the Recital (29) stated that "commercial communications are essential for the financing of information society services and for developing a wide variety of new, charge-free services".

298 Internet Provisions (网络规定) (n208), Art. 8.

299 *Han Han v. Baidu (韩寒v.百度)* (n42). In this case, one of Hanhan's works was illegally uploaded to the literature-sharing website operated by the defendant, Baidu, so Hanhan sued Baidu for copyright infringement. This was a high attention case in China. Han Han is one of most distinguished young writers, who has lots of fans in China, and in May 2010, he was named one of most influential people in the world by Time magazine. The other party, Baidu, can be seen as the Chinese Google, and is one of the most successful internet companies in China. Therefore, the dispute between these two parties attracted lots of attention, and finally this case was selected as one of ten annual IP cases (2012) by People's Supreme Court.

300 Io *Group, Inc. v. Veoh Networks, Inc.*(n5), at 1143, 1155.

over certain content in its service, even including manually checking this content.[301] Therefore, it is already out of date to restrict hosting ISPs with the requirement of pure passivity, and even for the purpose of reinforcing copyright protection, it is reasonable to allow hosting ISPs to do certain management on the uploads.

Then, what are the appropriate criteria for a qualified hosting ISP in the post-web 2.0 era? One should refer to the decision made by the ECJ (European Court of Justice) in the Google ad-words case, which stated as follows: "it is necessary to examine whether the role played by that service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores."[302] According to this statement, a hosting ISP is still qualified for protection under the "safe harbor provision" unless its management of uploaded content results in its knowledge or control of them. This criterion does allow hosting ISPs to engage in some management over uploaded content, but such management should not be too much, so as to prevent hosting ISPs from taking advantage of infringing content of which they are already aware. Besides, the criterion drawn from US case law[303] is also quite reasonable, namely, if the management of content benefits the prevention of infringements, this kind of management should be permissible. If the former criterion warns hosting ISPs how much management can be done, the criterion in the US tells hosting ISPs what kind of management can be done. The US criterion also wins support in the EU, and some stakeholders, especially the ISPs, tried to persuade the Commission to adopt the so-called "Good Samaritan clause", which would make sure that an ISP which voluntarily takes actions against infringement would in principle not be punished.[304]

Table 2*: relevant factors of assessing hosting ISPs' passivity in the US, EU and China

	Inserting Ads	Displaying logos	Rights transfer	Automatically editing	Manually editing	Self-uploading
US	×	×	×	×	√	×
EU					√	
China			×		√	×

* *This Table describes a general comparison on how the courts in the US, EU and China evaluate the factors relevant to decide whether a hosting ISP remains passive enough in operation. "√" means that the factor concerned has always been an important reason to disqualify a hosting ISP as not passive enough in this jurisdiction, and "×" means the opposite. "↘" means that the factor concerned was an important reason to disqualify the passivity of a hosting ISP, but is becoming less important nowadays in this jurisdiction.*

301 *See* BGH – Rapidshare (n42), at para. 58. In this case, the German Federal Court of Justice held that because the Rapidshare had induced copyright infringements committed in a substantial scale, it was reasonable for it to take comprehensive and regular control over link collections which referred to its service.

302 Ibid, at para. 114.

303 *See* the discussion about courts' interpretation about hosting ISPs' passivity made in Section 3.3.

304 Commission Staff Working Paper: Online Services, Including E-commerce in the Single Market (n37), at 36.

3.6 Conclusion

To sum up, apart from the US and UK where the courts set a quite low threshold for a hosting ISP to be a qualified entity falling under the "safe harbor" provisions, the courts in some EU Member States (Germany, France and Italy) and China had in a long period held a defendant not qualified as a hosting ISP for the reason of its lesser degree of passivity under the following circumstances: commercially exploiting the user generated content, editing or categorizing the uploaded content, displaying its logo with uploaded content, requiring rights transfer by "terms and conditions," or uploading some content by itself, which can be seen as certain management of uploaded content made by hosting ISPs. However, in the Web 2.0, it is no longer reasonable to require hosting ISPs to keep purely passive, and they should be allowed to conduct certain management on the uploaded contents. In order to draw a proper borderline for the permissible management, one needs to first check whether this management will result in its knowledge or control of uploaded content, and then check whether this management is conducive to the prevention of infringements or not. By following this criterion, generally the management discussed in Section 3.4 cannot function as the reasons to shut hosting ISPs out of the "safe harbor," except editing, categorizing, or actively exploiting the uploaded contents. This criterion not only allows hosting ISPs to manage uploaded content to optimize their services, but also prevents them from using infringing materials for profits, and even encourages them to adopt measures against infringement on their platforms; this book therefore asserts that it helps to maximize hosting ISPs' freedom to operate in the US, EU and China.

Chapter 4

Hosting ISPs' Secondary Liability under the Roof of "Safe Harbor" Provisions

Introduction:

The previous chapter discusses under what circumstances a hosting ISP meets the threshold of "safe harbor" provisions. This chapter will discuss how the courts in the US, EU and China to decide hosting ISPs' secondary liability under the roof of the "safe harbor" provisions. In the light of "safe harbor" provisions, a hosting ISP who complies with certain requirements can be exempted from paying monetary damages.[305] However, regarding the other kind of reliefs, such as injunction, "safe harbor" provisions cannot immunize hosting ISPs from them. Therefore, even though a hosting ISP fully complies with liability exemption conditions set in "safe harbor" provisions, it may still face liabilities other than paying monetary damages according to the traditional liability rules. Besides, as was mentioned in the end of chapter 2, when interpreting "safe harbor" provisions, the courts cannot avoid being affected by traditional liability rules, so even though the US, EU and China have reached certain harmonization in the respect of "safe harbor" provisions, in light of case law, the secondary liability rules of hosting ISPs are still diverse in the US, EU and China. This chapter will take a comparative approach to examine the hosting ISPs' secondary liability for copyright infringement on their platforms in the US, EU and China.

First, this chapter examines how the courts evaluate the relevant factors when deciding liability in the US, EU and China, including monitoring responsibility (4.1), specific knowledge of
86 infringement (4.2), measures against repeat infringement (4.3), benefit from infringement (4.4), and inducement (4.5). Then, it introduces the Chinese specific approaches to conclude hosting ISPS' liability (4.6). Based on the discussion in the previous parts, it summarizes and examines the tendencies of case law development in the US, EU and China, and concludes, for the purpose of maximizing the freedom to operate of hosting ISPs, how the relevant factors should be interpreted when deciding liability (4.7).

4.1 Monitoring Responsibility and General Knowledge of Infringements

With the development of Internet technologies, the public currently can easily upload videos, music and text on hosting ISP's platforms through their computers, pads or even cell phones. Facing such immense amounts of uploads every day, whether hosting ISPs need to undertake monitoring responsibility becomes a key question. If the answer is yes, hosting ISPs need to actively examine every upload so as to remove infringing materials, which seems quite burdensome for hosting ISPs. But if hosting ISPs do not need to monitor the uploads, lots of copyrighted contents will be uploaded on hosting ISPs' platforms, which seems unfair to copyright owners. In the following section, the relevant rules about monitoring responsibility in the US, EU and China will be discussed.

305 See DMCA (n1), Sec. 512, (c)(1); E-commerce Directive (n1), Art. 14; Internet Regulation (网络条例) (n1), Art. 22.

4.1.1 "No Monitoring Responsibility" Clause in the US

The "no monitoring responsibility" clause in Digital Millennium Copyright Act (DMCA) § 512 can be seen as offering a major concession to the ISPs, under which, an ISP does not need to "monitor its service or affirmatively seek facts indicating infringing activity,"[306] and it also functions as the backbone of "safe harbor" provisions. Furthermore, the "no monitoring responsibility" is closely related to another concept "general knowledge of infringements", which means that an ISP can be deemed to know definitely that some of its users transmit infringed content through the internet service it offers, but it does not know exactly which content transmitted by which users are infringing. By deducing from "no monitoring responsibility", the general knowledge of infringements cannot be understood as imputed knowledge in the context of DMCA §512. This is because if an ISP should be liable for its general knowledge of copyright infringement, then it must monitor its internet service to seek the infringers and to stop further copyright infringement, since it is highly likely the use of its service can cause copyright infringement. William Patry points out that, "as a result of this lack of any obligation to be pro-active in seeking out possible infringements, service providers cannot be tagged for imputed knowledge where there are infringing materials and the service provider does not take steps to identify or monitor such material," so the "no monitoring responsibility" clause thus functions as a significant limitation on imputed knowledge.[307] In the US, whether general knowledge of infringement would lead a third party who had sold neutral products to undertake secondary liability was settled in "*Sony Betamax*" case, which established a liability standard called "substantial non-infringing use" by referring to the "staple article of commerce" patent law doctrine.[308] According to this standard, if a product is capable of substantial non-infringing uses, its distribution cannot result in contributory liability, unless the distributor fails to take corresponding action once knowing about a specific instance of infringement.[309] This implies that a general knowledge of infringement alone will not result in secondary liability. From a legal perspective, the Internet service offered by ISPs is similar to the Betamax sold by Sony, both of which are capable of substantial non-infringing use, so the rationality embodied in the "*Sony Betamax*" case has also been merged into DMCA §512.

In brief, because of the "no monitoring responsibility" clause the courts in the US always refuse to enforce secondary liability against ISPs when the claim against them is based purely on the grounds of their general knowledge of infringement. In the case of *Capitol Records, Inc. v. MP3tunes, LLC*, the defendant MP3tunes was a

306 DMCA (n1), Sec. 512, (m)(1).
307 Patry, *Patry on Copyright* (n265), § 21:85.
308 See *Sony Corp. of America v. Universal City Studios, Inc.* (n27), at 442.
309 Ibid.

website allowing users to store music files into their personal online "lockers" in which the plaintiff claimed there were lots of files infringing its copyright, so the plaintiff sued the MP3tunes for copyright infringement.[310] The District Court of S.D. New York held that although the defendant definitely knew some level of infringement was occurring on its website, it did not have specific "red flag" knowledge of any particular infringing materials, so the defendant qualified for "safe harbor" in terms of DMCA 512(c)(1)(A).[311] In the case of *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, the defendant Shelter Capital Partners owned a video-sharing website called Veoh, and the plaintiff sued Veoh for copyright infringement based on claiming that some of its copyrighted music videos were uploaded on Veoh without its permission.[312] The Court of Appeals for the Ninth Circuit held that "a broad conception of the knowledge requirement" argued by the plaintiff was inappropriate, and only "specific knowledge of particular infringing activity" could shut Veoh out of the "safe harbor."[313] In the case of *Viacom v. YouTube*, the Court of Appeals of the Second Circuit reaffirmed the doctrine of requiring specific knowledge again and rejected the plaintiff's attempt to interpret the "red flag" standard as an indication basis to hold the ISP liable for its general knowledge of direct infringements.[314]

4.1.2 "No General Obligation to Monitor" Clause in the EU

88 In the EU, the Directive on Electronic Commerce provides similar rules about ISPs' monitoring responsibility: Member States must not impose a general obligation on providers, when providing the service covered by Article 12 (mere conduit), 13 (caching) and 14 (hosting), to monitor the information they "transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity."[315] In several cases about ISPs' liability heard by the ECJ, the ECJ reaffirmed that no general obligation should be allocated to ISPs.[316] Further, regarding the knowledge of infringement, as noted by Niilo Jääskinen, since Article 15 of E-Commerce Directive forbade the imposition of a general obligation on ISPs, "it is not enough that the service provider ought to have known or has good reasons to suspect illegal activity."[317] In member states, "no general obligation to monitor" clause has been incorporated into their national laws. For instance, in Germany, the "no general obligation to monitor" clause is transplanted into § 7 TMG (2), and thus, the German courts, by following this clause, conclude that the general knowledge of infringements does

310 *Capitol Records, Inc. v. MP3tunes, LLC*, 821 F.Supp.2d 627, at 633 (S.D.N.Y., 2011).
311 Ibid, at 644-645.
312 *UMG Recordings, Inc. v. Shelter Capital Partners LLC* (n269), at 1027-1028.
313 Ibid, 1037-1038.
314 See *Viacom International, INC. v. YouTube, INC.* (n7), at 30-31.
315 E-commerce Directive (n1), Art. 15.
316 C-360/10, *SABAM v. Netlog NV* [2012], ECLI:EU:C:2012:85; *Google France SARL and Google Inc. v Louis Vuitton Malletier SA and Others* (n230); C-324/09, *L'Oréal SA and Others v eBay International AG and Others*, [2011] ECR I-06011.
317 Opinion of Advocate General, case C 324-9 (n291), at para. 163.

not qualify as imputed knowledge. For example, in *Greatest Hits II*, the Regional Court of Düsseldorf held that "generic knowledge of infringing use is insufficient to trigger liability."[318] In *Rapidshare II*, the Higher Regional Court of Hamburg held that "infringing use was foreseeable and likely, but noted that unless the service provider willfully ignored it, specific knowledge was still required to impose contributory liability."[319] In France, the "no general obligation to monitor" clause is incorporated into LCEN.[320] In 2007, Dailymotion, a video-sharing website, was held as a publisher by District of Paris and thus liable because it generally knew that its platform was used for posting illegal contents.[321] But since 2008, Dailymotion was held as a competent hosting ISP by the French courts, and then did not need to be liable for its general knowledge of infringement anymore.[322]

4.1.3 From "Uncertainty" to "No General Monitoring" in China

In China, the People's Supreme Court had already used DMCA §512 as an important reference when it provided the first Interpretation about Hosting ISPs' liability;[323] however, for unknown reasons it did not integrate a "no monitoring responsibility" clause which is an essential provision in DMCA 512.[324] Six years later, unfortunately again, the Internet Regulation, which includes a Chinese version of "safe harbor" provisions, still did not address an ISP's monitoring responsibility, and this loophole has resulted in confusion about this issue in judicial practice. For example, in the case of "*vale.com v. tudou.com*", the Shanghai First Intermediate People's court concluded that the defendant, a video-sharing website operator, definitely knew that some of the works being uploaded by its users were infringing … so the defendant should have monitored the content uploaded by its users in order to filter out infringing content.[325] By contrast, in another case, "*Wangyajun v. Lingshida Tech.*", the court affirmed that the defendant, as an Internet platform offering information storing space, faced a huge volume of uploaded content each day, so that it was unreasonable to impose monitoring responsibility on it.[326]

318 LG Düsseldorf: Störerhaftung des Filesharing-Betreibers, 2008 MMR 759 (quoting S. Barazza, 'Secondary liability for IP infringement: converging patterns and approaches in comparative case law' (n118), at 885.

319 OLG Hamburg: Haftung eines Sharehosting-Dienstes für rechtsverletzende Inhalte - Rapidshare II, GRUR-RR 2012, 335, (quoting Ibid).

320 Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (n155), Art. 6-1-7.

321 Waisman A and Hevia M, 'Theoretical Foundations of Search Eengine Liability' (2011) 42 International Review of Intellectual Property and Competition Law 785, at 798.

322 Ibid.

323 See Internet Interpretation (2000) (网络解释(2000)) (n190), this Judicial Interpretation brought in a "notice-delete" mechanism and subpoena calling for information to identify infringers from DMCA 512.

324 Ibid, the Judicial Interpretation did not address the issue of an ISP's monitoring responsibility.

325 *vale.com v. tudou.com (网乐互联v.土豆网)*, Shanghai First Intermediate People's Court (上海市第一中级人民法院), No. 19 Hu Yi Zhong Min Wu (Zhi) Zhong Zi (2009) (（2009）沪一中民五（知）终字第19号).

326 See *Wangyajun v. Lingshida Tech. (王亚军v.北京零时达科技)*, Beijing Haidian District Court (北京市海淀区人民法院), No. 2775 Hai Min Chu Zi (2008) (（2008）海民初字第2775).

With the studies about ISPs' secondary liability arising in China, especially after many judicial decisions in the EU and US have been introduced into China, a consensus of no monitoring responsibility has been gradually reached in China. As stated by an official from the People's Supreme Court, in the US and EU, it is a common practice that ISPs have no obligation to monitor overwhelming amounts of content on the Internet.[327] In 2012, the National Copyright Administration in China published two revised drafts of the proposed Copyright Law, both of which include an article which clearly states that if an Internet service provider offers storage, search, linking or other purely technical services to Internet users, then it is not obliged to monitor the information concerning copyright or related rights.[328] Furthermore, the recently promulgated Interpretation also provides that where an internet service provider does not take the initiative to monitor the Internet users' infringement of the right to Network dissemination of information, the People's courts shall not conclude that it is at fault for allowing primary infringement to occur.[329] Since then, it has been officially rejected that the ISPs' general knowledge of primary copyright infringement can result in secondary liability, and thus Chinese jurisdictions began to conform to prevailing practices in the US and EU in this respect.

4.2 Specific Knowledge of Infringements

90 Specific knowledge is a concept which is related to general knowledge but with a different meaning from the legal perspective. As its name implies, unlike general knowledge, specific knowledge requires more than having a general awareness that infringements are occurring, but rather a precise knowledge that a particular incident of infringement has occurred. The US, EU, and China, all recognize that if an ISP possesses specific knowledge of infringement but does not expeditiously stop it, then it should be secondarily liable for these acts of infringements. As provided in DMCA §512(c)(1)(A), in order to avoid monetary damages, the hosting ISP must not "have actual knowledge that the material or an activity using the material on the system or internet is infringing; in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the material."[330] The relevant provision in the EU Directive on electronic commerce is quite similar to the DMCA provision. The EU Directive

327 This statement was presented at a press conference on introducing "The Provisions of the Supreme People's Court on Several Issues Concerning Application of Law in the Trial of Cases Involving Disputes about Infringing Right to Internet Dissemination of Information (2013)" when the official was questioned about "ISPs' monitoring liability", http://www.sipo.gov.cn/mtjj/2013/201301/t20130121_783586.html (last visited 18-09-2014).

328 People's Republic of China Copyright Law (first revising draft), Art. 69, published by National Copyright Office in March, 2012. In second revising draft, the same rule is also provided in Article 69.

329 Internet Provisions (网络规定) (n208), Art. 8.

330 DMCA (n1), Sec. 512 (c) (1) (A).

provides that if the hosting ISP does not "have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; and upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the information."[331] In member states, this provision has been incorporated into their national laws. In China, the knowledge requirement for ISP liability immunity is articulated slightly differently from the provisions in the US and EU, and it reads as follows: "the (hosting) ISP has no knowledge of and no justifiable reason to know the infringement of the works, performance, sound or video recordings."[332] From the above provisions, it is clear that "specific knowledge" can be categorized into two types of knowledge, actual knowledge and constructive knowledge.

4.2.1 "Red flag" Standard in US

"That actual knowledge standard is high, and by itself does not reach an entity that willfully ignores blatant indications of infringement,"[333] which means actual knowledge is difficult to prove. Therefore, the parties involved always argue about what constitutes constructive knowledge of an infringing activity. According to the House Report (commerce committee), the provisions about constructive knowledge in DMCA can best be described as a "red flag" test, which means if the service provider becomes aware of a "red flag" from which infringing activity is apparent, it will lose the limitation of liability if it takes no action.

> The "red flag" test has both a subjective and an objective element. In determining whether the service provider was aware of a "red flag", the subjective awareness of the service provider of the facts or circumstances in question must be determined. However, in deciding whether those facts or circumstances constitute a "red flag", in other words, whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances, an objective standard should be used.[334]

In the view of David Nimmer, the knowledge requirement required by the "red flag" test is more favorable to ISPs than the previous contributory infringement, which is not "what a reasonable person would have deduced given all the circumstances, but rather whether the service provider deliberately proceeded in the face of blatant factors of which it was aware,"[335] so as to "avoid rewarding those (ISPs) who adopt the posture of an ostrich."[336] In other words, the infringing flag must be "brightly

331 E-commerce Directive (n1), Art. 14, 1.
332 Internet Regulation (网络条例) (n1), Art. 22 (3).
333 Nimmer D, *Copyright: Sacred Text, Technology, and the DMCA*, (Kluwer Law International, 2003), at 358.
334 H.R. REP. 105-551(II) (n16), at 53.
335 See Nimmer, *Copyright: Sacred Text, Technology, and the DMCA* (n328), at 358.
336 Ibid.

red indeed--and be waving blatantly in the provider's face--to serve the statutory goal of making 'infringing activity ... apparent.'"[337] Nimmer's interpretation of the "red flag" test has been widely quoted by the US courts.[338] As for what constitutes "red flag", the legislative history suggests a high standard:

> The infringing nature of such sites shall be apparent from even a brief and casual viewing, e.g., sites typically use words such as 'pirate', 'bootleg', or slang terms in their URL and header information to make their illegal purpose obvious … to internet users; but just one or more well known photographs of a celebrity at a site cannot be treated as red flag.[339]

By following this high standard, the US courts held that the following circumstances did not qualify as a "red flag": 1) if investigation of "facts and circumstances" is required to identify material as infringing, then those facts and circumstances are not "red flags";[340] 2) hosting of password-hacking websites is not a per se "red flag" of infringement;[341] 3) the disclaimer, which states that "copyrights of these files remain the creator's. I do not claim any rights to these files, other than the right to post them" was not a "red flag" of infringement;[342] 4) describing photographs as "illegal" or "stolen" is not "red flag";[343] the professionally created nature of uploaded content does not constitute per se a "red flag" of infringement.[344] However, a notification about specific infringement from a third party, such as an Internet user, rather than from a copyright owner, might meet the "red flag" test.[345] The case law in the US

337 Ibid.

338 See *Io Group, Inc. v. Veoh Internets, Inc.* (n5), at 1148; *Corbis Corporation v. Amazon.com*, 351 F.Supp.2d 1090, at 1108 (W.D. Washington 2004).

339 See H.R. REP. 105-551(II) (n16), supra note 21, at 57-58.

340 *UMG Recordings, Inc. v. Veoh Internets, Inc.* (n275), at 1108.

341 *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, at 1114 (9th Cir. 2007). As stated by the court, the burden of determining whether passwords on a website enabled infringement is not up to the service provider. The website could be a hoax, or out of date. The owner of the protected content may have supplied the passwords as a short-term promotion, or as an attempt to collect information from unsuspecting users. The passwords might be provided to help users maintain anonymity without infringing copyright. There is simply no way for a service provider to conclude that the passwords enabled infringement without trying the passwords, and verifying that they enabled illegal access to copyrighted material. We impose no such investigative duties on service providers.

342 Ibid. As stated by the court, contrary to Perfect 10's assertion, this disclaimer is not a "red flag" of infringement. The disclaimer specifically states that the webmaster has the right to post the files.

343 Ibid. As stated by the court, describing photographs as "illegal" or "stolen" may be an attempt to increase their salacious appeal, rather than an admission that the photographs are actually illegal or stolen, and shouldn't place the burden of determining whether photographs are actually illegal on a service provider.

344 *Io Group, Inc. v. Veoh Internets, Inc.* (n5), at 1149. As stated by the court, with the video equipment available to the general public today, there may be little, if any, distinction between "professional" and amateur productions.

345 *UMG Recordings, Inc. v. Shelter Capital Partners LLC* (n269), at 1040. In this case, the Court made a very interesting differentiation between the notifications from a copyright owner and the third party. The CEO of Disney sent an email to a Veoh investor, which stated that the movie Cinderella III and various episodes were available on Veoh without Disney's authorization. The court decided that this email did not qualify as a red flag for the following reason: as a copyright holder, Disney was subject to the notification requirements in § 512(c)(3), which this informal email failed to meet. However, if this notification had come from a third party, such as an Internet user, it might meet the "red flag" test, since it specified particular infringing material.

examining facts, such as hosting of password-hacking websites, statement of right disclaimer, describing content as "illegal" or "stolen", which always indicates the illegal nature of content, finding that these circumstances do not establish a red flag suggests that establishing a red flag is a very high burden for any copyright owner alleging infringement.

Even though the US courts recognize the existence of "red flag", an ISP will not definitely possess "red flag" knowledge, because another subjective requirement still needs to be met, namely, the ISP shall subjectively know the existence of "red flag", which is also hard to prove. As Judge Howard stated in the case of "*Io v. Veoh*", "although one of the works did contain plaintiff's trademark several minutes into the clip (which might qualify for red flag), there is no evidence from which it can be inferred that Veoh was aware of, but chose to ignore, it."[346] First, the percentage of infringing content on hosting platform is irrelevant to the specific knowledge. In the case of *Viacom v. YouTube*, the evidence cited by the plaintiff Viacom indicated that YouTube knew about 75-80% of its streams containing copyrighted materials, and "more than 60% of YouTube's content was "premium" copyrighted content" but only 10% of it was authorized.[347]However, the court held that these statements were not sufficient, standing alone, to result in YouTube's specific knowledge of any instance of infringement from the legal perspective.[348] Second, hosting ISPs should bear specific knowledge of infringing materials in the litigation rather than other infringing materials. In the case of *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, the court held that even if the defendant's knowledge of materials that infringed Disney's movies and TV shows qualified for the "red flag" test, this fact would not favor the plaintiff's claims that the defendant knowingly hosted unauthorized music videos from UMG.[349] In the case of *Viacom v. YouTube*, although the plaintiff successfully demonstrated that YouTube knew some particular infringing video clips, the court held that "only the current clips-in-suit are at issue in this litigation."[350] Further, hosting ISPs' confession, such indicating the knowledge of particular infringement in internal reports and email exchanges, can provide strong evidence for a "red flag." In the case of *Viacom v. YouTube*, an internal report from YouTube stated that there were episodes and clips of some well-known shows which were blatantly illegal on YouTube, and some internal e-mail exchanges also indicated that YouTube knew of the particular infringing video on its platform, so the Court concluded that YouTube bore specific knowledge of infringing videos indicated in the report and e-mail exchanges.[351] However, normally this kind of internal document is

346 See *Io Group, Inc. v. Veoh Internets, Inc.* (n5), at 1149.
347 See *Viacom International, INC. v. YouTube, INC.* (n7), at 33.
348 Ibid.
349 *UMG Recordings, Inc. v. Shelter Capital Partners LLC* (n269), at 1040.
350 See *Viacom International, INC. v. YouTube, INC.* (n7), at 34.
351 Ibid.

out of the reach of copyright owners. Therefore, constructive knowledge of a hosting ISP is not easy to establish through applying the "red flag" test. Besides the "red flag" test provided in DMCA §512, according to the common law, willful blindness is tantamount to knowledge.[352] Therefore, willful blindness can also lead to ISPs being liable for the primary infringement committed by its users. By referring to case law, one can find that a person is "willfully blind" if the person is "aware of a high probability of the fact in dispute and consciously avoided confirming that fact."[353] From this definition, it appears that the liability resulting from "willful blindness" can be based on a defendant's general knowledge of infringement (aware of a high probability of the fact in dispute). However, as mentioned before, the "no monitoring responsibility" clause in DMCA §512 prohibits a court from concluding secondary liability based on an ISP's general knowledge of infringement.[354] Therefore, when applied to a hosting ISP's liability, the doctrine of "willful blindness" should be strictly interpreted. As for how strictly it should be, in a case, the US District Court for Southern District of New York held that what disqualifies the service provider from DMCA§512 protection is blindness to "specific and identifiable instances of infringement."[355] The court's interpretation turns the "willful blindness" test back to an analysis of the "red flag" test; because, the red flag should be a specific and identifiable instance of copyright infringement. If so, then the "willful blindness" doctrine seems no more than to reaffirm the "red flag" test. However, in the long term, more relevant case law is needed to determine how precisely "willful blindness" should be applied.

94

4.2.2 Hosting ISPs' Specific Knowledge in the EU

According to Article 14 of E-Commerce Directive, in order to benefit from liability exemption, hosting ISPs should "not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent;" or "upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."[356] With regard to actual knowledge, the E-Commerce Directive is silent on what constitutes actual knowledge, and "leaves it for courts

352 *Tiffany (NJ) Inc. v. eBay, Inc.*, 600 F.3d 93, at 110 (2d Cir. 2010).

353 *United States v. Aina-Marshall*, 336 F.3d 167, at 170 (2d Cir. 2003) (quoting *United States v. Rodriguez*, 983 F.2d 455, at 458 (2d Cir.1993)).

354 See *Viacom International, INC. v. YouTube, INC.* (n7), at 35. As stated by the Federal Court of Second Circuit, Section 512(m) is explicit: DMCA safe harbor protection cannot be conditioned on affirmative monitoring by a service provider. For that reason, § 512(m) is incompatible with a broad common law duty to monitor or otherwise seek out infringing activity based on general awareness that an infringement may be occurring.

355 *Viacom Int'l Inc. et al. v. YouTube et al.*, 07 civ. 2103 (LLS), 32 (S.D.N.Y. Apr. 18, 2013)

356 E-commerce Directive (n1), Art. 14.

to decide the levels and types of knowledge that actual knowledge requires."[357] As for awareness of apparent infringement, it should be understood to be as same as "should have known" and "have reason to know" which are applied in tort law for the purpose of evaluating constructive knowledge.[358] In the case of *L'Oréal v. eBay*, the ECJ provided some clues to decide whether a hosting ISP had knowledge of infringement prescribed in Article 14.[359] According to the ECJ's decision in this case:[360]

> it is sufficient, in order for the provider of an information society service to be denied entitlement to the exemption from liability provided for in Article 14 of Directive 2000/31, for it to have been aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality in question and acted in accordance with Article 14(1)(b) of Directive 2000/31.

So, when deciding whether a fact or circumstance can lead to a hosting ISP's knowledge of illegal information or activity, the court should treat the hosting ISP as a diligent economic operator. If from the perspective of a diligent economic operator, the illegality of information or activity is apparent from the fact or circumstance, the court should hold that the hosting ISP concerned knows about the infringement. Regarding how a hosting ISP can know the aforesaid facts or circumstances, the ECJ further stated that:[361]

> The situations thus covered include, in particular, that in which the operator of an online marketplace uncovers, as the result of an investigation undertaken on its own initiative, an illegal activity or illegal information, as well as a situation in which the operator is notified of the existence of such an activity or such information. In the second case, although such a notification admittedly cannot automatically preclude the exemption from liability provided for in Article 14 of Directive 2000/31, given that notifications of allegedly illegal activities or information may turn out to be insufficiently precise or inadequately substantiated, the fact remains that such notification represents, as a general rule, a factor of which the national court must take account when determining, in the light of the information so transmitted to the operator, whether the latter was actually aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality.

357 Sadeghi M, *The Knowledge Standard for ISP Copyright and Trademark Secondary Liability: A Comparative Study on the Analysis of US and EU Laws* (Brunel University London, 2013), at 103.

358 Larusdottir JS, 'Liability of Intermediaries for Copyright Infringement in the Case of Hosting on the Internet' (2004) 47 Scandinavian Studies in Law 471, at 484.

359 *L'Oréal SA and Others v eBay International AG and Others* (n327).

360 Ibid, para. 120.

361 Ibid, para. 122.

Therefore, a hosting ISP can acquire such facts or circumstances in various ways, including through its own investigation and being notified by copyright owners. In this case, the ECJ created a new notion "a diligent economic operator" for deciding whether a hosting ISP knows the illegal nature of infringing materials, but did not provide a definition for this notion, which leaves much space for Member States to interpret. Further, before evaluating the illegal nature of infringing materials, hosting ISPs have to know the infringing materials concerned at the first place, and the ECJ held that the knowledge as such can be acquired through either their own investigation or notifications from rights holders. In the following text, it explores how this knowledge standard in Article 14 is implemented in several member states.

4.2.2.1 Positive Knowledge in Germany

In Germany, "actual knowledge" is called "positive knowledge" (positive Kenntnis).[362] According to the dominant legal opinion, positive knowledge of concrete and specified information should be understood in terms of direct intent (dolus directus);[363] this means that "should know" in the sense of rough negligence is not enough to constitute positive knowledge.[364] Therefore, it is common for the German courts to conclude that negligent ignorance is not equal to the positive knowledge required by law.[365] However, a hosting ISP cannot be completely
96 immunized from monetary claims if it does not know of the infringements by reason of its rough negligence, because under Article 10 of German TMG, in order to enjoy the immunity, a hosting ISP should not know any fact or circumstance from which the illegality of the conduct or information is apparent.[366] Nevertheless, the rough negligence provided in TMG § 10 limits its application only to deliberately rough negligence, and can only be found in clear and obvious cases,[367] such as where the concrete evidence of committing definitely illegal conduct or absolutely illegal content is displayed in front of the hosting ISP.[368]

The TMG § 10 includes the language "keine Kenntnis von der rechtswidrigen Handlung oder der information", which was inherited from § 5 of the 1997 TDG and can be translated in English as "no knowledge of the illegal conduct or the information". However, in the German language context, it can be interpreted in two ways, one of which is "no knowledge of the illegal conduct and no knowledge of illegal information" and the other being "no knowledge of the illegal conduct

362 Fitzner, *Von Digital-Rights-Management zu Content Identification: neue Ansätze zum Schutz urheberrechtlich geschützter Multimediawerke im Internet: eine tec*h*nische, ökonomische und rechtliche Analyse* (n268), at 283.

363 Ibid.

364 OLG München: Gewerbeschädigende Äußerungen in einem Meinungsforum im Internet, 2002 MMR 612.

365 Spindler, et al., *Rec*ht *der elektronischen Medien: Kommentar* (n268), at 1530.

366 Telemediengesetz (TMG), Sec. 10(1).

367 See Fitzner, *Von Digital-Rights-Management zu Content Identification: neue Ansätze zum Schutz urheberrechtlich geschützter Multimediawerke im Internet: eine technische, ökonomische und rechtliche Analyse* (n268), at 287.

368 LG Düsseldorf: Markenrechtsverletzung durch Onlineauktion, 2003 MMR 120-127.

and no knowledge of information." There has been considerable disagreement as to how TDG §5 should be interpreted. According to the German legislators, the term "illegal" in Article 14 of ECRL only points to conduct but is irrelevant to interpreting the term "information," so for the "information," the knowledge requirement can be fulfilled if the hosting ISP knows the existence of the information regardless of whether it also knows the illegality of this information or not.[369] However, Prof. Spindler believes that the German legislators unintentionally misunderstood Article 14 of the ECRL when transplanting it into German law; on the contrary, the ECRL does not differentiate between conduct and information with regard to illegality.[370] The circumstances are, however, different. For example, in the case of illegal conduct, the information itself is legal, and only the conduct such as the unauthorized copying or publishing of this information is illegal; in the case of illegal information, the information itself is illegal, such as pornography, violent or Nazi content.[371] After the "*Google AdWords*" case concluded by the ECJ, the debate about this question seemed to end, because the ECJ had specifically declared that a service provider cannot be held liable for data which it has stored at the request of an advertiser, unless, it had knowledge of the unlawful nature of the data or of the advertiser's activities, but failed to act expeditiously to remove or to disable access to the data concerned.[372] A month later, the German Federal Court of Justice followed the ECJ's opinion in the case of "*Google AdWords*",[373] and since then in Germany a hosting ISP must have knowledge of the illegality of information in order to trigger its responsibility to delete or block this information. 97

With development of filtering technologies, many hosting ISPs have installed filtering programs in order to reduce copyright infringement. Before any content can be uploaded, it will be scanned by the filtering program, so technically this content is known by the filtering program. This raises the question of whether the information that is "known to" a filtering program is legally equated to the knowledge possessed by the hosting ISP. The "knowledge" of the filtering program if attributed to the ISP may remove the hosting ISP from of its "safe harbor". It is generally accepted that, because a hosting ISP not only needs to know the information but also the illegality of the information, and the machine cannot displace the human in checking whether the information is infringing or not, then the knowledge of the filtering program should not be seen as fulfilling the knowledge in the sense of TMG § 10.[374]

369 BT-Drs. 14/6098, S. 25, (quoting Spindler, et al., *Recht der elektronischen Medien: Kommentar* (n268), at 1531.)

370 See Spindler, et al., *Recht der elektronischen Medien: Kommentar* (n268), at 1531.

371 Ibid.

372 *Google France SARL and Google Inc. v Louis Vuitton Malletier SA and Others* (n230), at Para. 120.

373 BGH, April 29, 2010, Case No. I ZR 69/08 – Vorschaubilder.

374 See Spindler, et al., *Recht der elektronischen Medien: Kommentar* (n268), at 1531-1532. Also see Fitzner, *Von Digital-Rights-Management zu Content Identification: neue Ansätze zum Schutz urheberrechtlich geschützter Multimediawerke im Internet: eine technische, ökonomische und rechtliche Analyse* (n268), at 289-290.

Generally speaking, it is not easy to prove that a hosting ISP has knowledge of copyright infringement as understood in TMG § 10. As noted by Prof. Hoeren, if there is no notification of an alleged infringement, then it is legally presumed that the provider has no sufficient knowledge of any infringing action and, consequently, the ISP is not responsible.[375]

4.2.2.2 Actual Knowledge in France

For the purpose of implementing the E-commerce Directive, in 2004, the law makers enacted the Act on Confidence in Digital Economy (LCEN). With regard to Hosting ISPs' liability, the LCEN reads almost the same as that in the E-commerce Directive, according to which, a hosting ISP is liable for the infringing contents uploaded by their users in the following circumstances: "it has actual knowledge of the illegal nature of stored content or of facts and circumstances showing its illegal character," and "upon obtaining such knowledge, it does not act expeditiously to remove or disable access to the data."[376] Therefore, hosting ISPs can only be held liable when they have actual knowledge of infringement on their platform and refuse to get rid of the infringement. As referred to before in the US part, actual knowledge is really hard to be proved, and normally only a competent notice can lead to the hosting ISP's knowledge of infringement. In order to increase the legal certainty, Article 6-5 of LCEN introduces
98 a notice procedure which rules on what kind of elements should be included in a notice.[377] Regarding how the case law in France interprets Article 6-5 and what kind of notice can lead to hosting ISPs' having actual knowledge, will be discussed in the next chapter. Anyhow in France, without receiving competent notices, hosting ISPs should not be considered to have actual knowledge of infringement.[378]

4.2.2.3 Knowledge in the UK

In the UK, for the purpose of implementing the E-Commerce Directive, the Electronic Commerce (EC Directive) Regulations 2002/2013 were enacted in 2002, and Article 19(a) literarily copied the knowledge criteria set in E-Commerce Directive.[379] Generally, in order to result in a hosting ISP's actual knowledge of infringement, a competent notice under Article 22 should be sent to the hosting ISP.[380] In the case of *McGrath v. Dawkins and Amazon*, Amazon was an online

375 Hoeren T and Yankova S, 'The Liability of Internet Intermediaries-The German Perspective' (2012) 43 International Review of Intellectual Property and Competition Law 501, at 510.

376 Nérisson, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in France' (n103), at 70.

377 LCEN, Art. 6-5, quoting ibid, at 71.

378 Ibid, at 71.

379 Electronic Commerce (EC Directive) Regulations 2002 (n155), Art. 19.

380 Lucy Nunn, *Internet service providers: copyright infringement*, Thomson Reuters(2014), *available at* http://login.westlaw.co.uk/maf/wluk/app/document?src=doc&linktype=ref&context=23&crumb-action=replace&docguid=I4B88A580587211E4B6DA87DCBE8E5CD8 (last visited 14-05-2014).

bookseller, and on its website the public could write a review of each book.[381] McGrath wrote a book concerning debate on religion versus science, and in order to publicize his book, he posted the details of it in a review of another writer's book on the Amazon' website, which aroused lots of critics of McGrath, and some of them were even hostile.[382] After receiving notice from McGrath, Amazon deleted some of the inappropriate items but not all of them, so McGrath sued Amazon for infringement.[383] When deciding whether Amazon could rely on defenses under Article 19 of the Electronic Commerce (EU Directive) Regulations 2002, the court held that Amazon, as a corporation, could only have actual knowledge of defamation through human representatives, and given the large scale of Amazon's website, it was impossible to know the posting in question before receiving the complaints from McGrath.[384] However, in this case, the complaining notice sent by McGrath was incompetent, so Amazon should not be held as knowing the postings in question.[385] Regarding constructive knowledge, it can be concluded that, if a hosting ISP is "aware of facts or circumstances from which it would have been apparent", then the activity was unlawful, but so far, no case laws offer further guidance on this point.[386]

4.2.2.4 Actual Knowledge in Italy

The E-commerce Directive was implemented in Italy through enacting the Legislative Decree 70/03 (thereafter "L.D 70/03"). In line with Article 16 of L.D. 70/03, in order to enjoy the liability exemption, a hosting ISP should not "have actual knowledge of unlawful activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the unlawful activity or information is apparent."[387] Besides, "upon obtaining such knowledge or awareness and upon communication of a court or of a competent authority, the provider acts expeditiously to remove or to disable access to the information."[388] As noted by Alberto Bellan, unlike what is provided in the E-commerce Directive, in Italy, it seems that besides having knowledge of infringement, an order from the court or a competent authority is still necessary to trigger the hosting ISPs' obligation to expeditiously remove the infringing materials in question.[389] With regard to the knowledge of infringement, according to Italian case law, whether a hosting ISP actually knows the infringement mainly relies on the notices sent

381 *McGrath v Dawkins and Amazon*, [2012] EWHC B3 (QB), para. 3.
382 Ibid, para. 4 and 5.
383 Ibid, para. 13 and 14.
384 Ibid, para. 42.
385 Ibid, para. 47.
386 Nunn, Internet service providers: copyright infringement (n375).
387 Art. 16(1) L.D. 70/03, quoting Bellan, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in Italy' (n238), at 90.
388 Ibid.
389 Ibid. More details will be discussed in the chapter "notice-and-takedown procedure in the US, EU and China."

by copyright owners.[390] As for what kind of information should be included in a notice so as to lead to the hosting ISP's actual knowledge, different courts made different opinions on this issue, which will be discussed in the next chapter. To sum up, at EU level, the ECJ held that when deciding whether a hosting ISP knew the illegality of information or activity, the court should treat the hosting ISP as a diligent economic operator.[391] Further, in order to conclude that the hosting ISPs had knowledge under Article 14 of E-Commerce Directive, the hosting ISPs should know the information or activities concerned in the first place and such knowledge can be acquired through either self-investigation or notification from rights holders.[392] Since hosting ISPs do not need to actively seek the infringing information or activities,[393] the notifications from copyright owners become the main source of the hosting ISPs' knowledge of infringement. As demonstrated by case law in the four Member States discussed above, before a competent notice has been sent, it usually cannot be concluded that the hosting ISP is aware of the infringement. Therefore, complaining notices play an important role in leading to the hosting ISP's knowledge of infringement in the EU.[394]

4.2.3 "Should Know" in China

In China, a hosting ISP's actual knowledge of infringement can rarely be proved,
100 except where it receives official notice from the copyright owner by post, fax or email to complain about the infringement.[395] As for what constitutes "should know", namely "justifiable reason to know" as provided in Internet Regulation, some Chinese courts have concluded the existence of "red flags" as being equivalent to "should know". In the case of *Hua Xia Shu Ren v. Youku.com*, the Handian District Court concluded that the defendant, "Youku.com", should have known of the infringements involved based on the following facts: 1) a large number of infringing videos, most of which were marked "copyright is reserved by Hua Xia Shu Ren", were claimed to be offered by an internet user, the so-called "Qilingjiao"; 2) the defendant also publicized its service as "Youku is a good learning club".[396] In this case, the videos marked "copyright is reserved by Hua Xia Shu Ren" can be treated as a qualified "red flag" in the context of the US "red flag" test, because the claim of "copyright reservation"

390 Bellan, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in Italy' (n238), at 112.

391 *L'Oréal SA and Others v eBay International AG and Others* (n327), at para. 120.

392 Ibid, at para. 121 and 122.

393 E-commerce Directive (n1), Art. 15.

394 In other member states, notices also play a vital role in resulting in hosting ISPs' knowledge of infringing materials. See Verbiest T et al., Study on the Liability of Internet Intermediaries (2007), at 36-46, *available at* http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf (last visited 28-08-2015).

395 See Internet Provisions (网络条例) (n208), Art. 13.

396 *Hua Xia Shu Ren v. Youku.com (华夏树人v.优酷)*, Beijing Haidian District Court (北京市海淀区法院), No. 9200 Hai Min Chu Zi (2008) (（2008）海民初字第9200号).

has already made the infringing nature of relevant videos obvious, just like the clip containing the plaintiff's trademark for several minutes in the case of *Io v. Veoh*[397]. *However, rather than applying both aspects of the US "red flag" test, the Handian District Court decided the question of liability without considering whether the defendant knew of the "red flag". Thus, the Handian District Court made hosting ISPs more easily subject to secondary liability than they would be under the two pronged "red flag" test in the US.*

Thereafter, scholars in China increasingly proposed the US "red flag" test, especially, Prof. Wang Qian, systematically started to advocate the implementation of the US "safe harbor" provisions in China, and wrote several influential articles about the US "red flag" test.[398] *Eventually, the Chinese courts determined that the application of the "red flag" test consists of two steps, one of which is the existence of "red flag", and the other is that a hosting ISP also knows of the "red flag". According to the Internet Provision issued by the People's Supreme Court, some factual circumstances under which a hosting ISP would be found to meet the "should know" standard are: 1) hot-play audio-video located on the homepage, other main pages, or other places of a website which can be easily identified by ISPs; 2) taking the initiative to choose, edit, sort or recommend the hot-play audio-video works, or setting a special top list for them; 3) other circumstances under which it can be easily determined that the relevant works, performances, audio recordings and sound or video recordings are offered without authorization, but the ISPs then failed to take reasonable measures to prevent the copyright infringement.*[399]

After examining the specific circumstances enumerated above in the Internet Provision, the shadow of the American "red flag" test can clearly be seen. The first circumstance demonstrates a concrete example fulfilling the "red flag" test. To be more precise, in terms of hot-play[400] audio-video works available on the Internet for free, hosting ISPs should know that these works are infringing copies without need of further investigation, since the copyright owners would not make their popular audio-video works available on the Internet without charge when these works are still considered hot-play. Therefore, these infringements are sufficient to qualify them as "red" flags. Furthermore, during their daily operations, the ISPs certainly check their own homepage and other main pages, so if these infringed

397 See *Io Group, Inc. v. Veoh Internets, Inc.* (n5), at 1149. In the decision, the court did not directly conclude that the clip qualified for "red flag", but it can be implied from the phrasing: "Although one of the works did contain the plaintiff's trademark several minutes into the clip, there is no evidence from which it can be inferred that Veoh was aware of, but chose to ignore, it."

398 Wang Q (王迁), 'Infringement Research on Copyright of Video-sharing Website (视频分享网站著作权侵权问题研究)' (2008) 4 Studies on Law and Business 42 (《法商研究》2008年第4期), at 42-53.

399 See Internet Provisions (网络规定) (n208), Art. 12.

400 "hot-play" is a term that can always be found in the decisions made by Chinese courts, and finally was incorporated into the Provisions by the People's Supreme Court. In terms of relevant decisions, "hot-play" has always been used to describe the audio-video works which are newly distributed, popular and still on screen.

hot-play audio-videos are being shown on these sites, the hosting ISPs cannot deny knowing these are flashing "red flags". For the second one, the facts depicted by it look more like direct infringements rather than indirect infringement subject to the "red flag" test, because if the hosting ISPs take the initiative to choose, edit, sort or recommend the hot-play audio-video works, they are actively involved in these infringements and should be defined as direct infringers rather than secondary or contributory infringers. Nevertheless, if they are actively participating in the copyright infringement, they clearly should know the infringement is taking place. The third circumstance can be seen as a substantial copy of the "red flag" test but expressed from another perspective.

Besides setting specific "should know" circumstances for hosting ISPs, concerning all types of ISPs, the Internet Provisions also list some others factors which need to be comprehensively assessed when concluding "should know". These are: 1) the character of service offered by ISPs, the ways of offering service, the possibility of leading to infringements through its service, and ISPs' capability of managing information; 2) the types and fame of transmitted works, performances, sound recordings and video recordings, and whether the infringement is obvious or not; 3) whether the ISPs take initiative to choose, edit, modify and recommend the works, performances, audio recordings and audio-video recordings; 4) whether the ISPs adopt reasonable measures to prevent infringements actively; 5) whether the ISPs set convenient processes to receive the infringing notices, and whether the ISPs respond to them reasonably; 6) whether the ISPs take reasonable responding measures against repeat infringements committed by the same internet user; 7) the other elements which need to be considered.[401]

By analyzing the factors enumerated above, one can find that, compared to the "red flag" test, they seem more likely to regulate the commercial model of ISPs rather than focus on whether the ISPs know about the existence of concrete infringement. Except for the second and third factors, which are directly relevant to the knowledge of ISPs, the other factors require the ISPs to fulfill a certain duty of care so as to reduce infringement. In addition, the People's Supreme Court also enumerates a particular instance, under which the People's courts can legally presume that the ISPs have knowledge that their Internet users are infringing a copyright owner's right to network dissemination of information, as follows: where the ISPs recommend the hot-play audio-video works by means of setting list, content, indexes, describing paragraph, content introduction, etc., when offering Internet service, and the public can access these works through directly downloading, browsing or other ways.[402]

401 See Internet Provisions (网络规定) (n208), Art. 9.
402 Ibid, Art. 10.

Based on the similar reasons referred to before, this particular instance is more like a direct copyright infringement rather than an indirect infringement, because if an ISP recommends any audio-video works, these audio-video works can be seen as being its own offering from a legal perspective, and thus it should be subject to direct liability, if there is any copyright infringement.

Based on the above discussion of imputed knowledge, one can find that, compared with judicial practice in the US, the Chinese courts seem to be interpreting imputed knowledge more broadly and extending it to cover not only the "red flag" test, but also to cover direct infringement. More importantly, the "should know" criterion in China compels hosting ISPs to undertake certain duties so as to regulate their business model. In contrast to what occurs in China, it seems that in the EU member states discussed above, the imputed knowledge can be found by the courts in quite limited circumstances, such as where competent notices have been sent by copyright owners.

4.3 Repeating Infringements

Since hosting ISPs do not need to undertake general monitoring responsibility for checking the content uploaded by their users, copyright owners rely heavily on certain ex post facto measures to protect their rights, such as measures against repeating infringements. In each country there are different measures required against repeating infringements. In the US, the "safe harbor" provisions require hosting ISPs to take necessary measures against repeat infringers. In the EU, although the E-Commerce Directive does not include a specific provision that requires hosting ISPs to prevent repeating infringements, it does indicate that the injunctions can be ordered by courts or authorities to require the termination or prevention of any infringement.[403] In China, the Internet Provision issued by the People's Supreme Court seems to adopt a mixed solution, which means hosting ISPs are required to take necessary measures against both repeat infringers and repeated infringement of the same copyrighted content. In this section, it discusses and compares the hosting ISPs' obligations against repeating infringement in the US, EU and China.

4.3.1 Repeat Infringer Policy in US

In the US, in order to enjoy liability limitation, an ISP should "have adopted and reasonably implemented, and informed subscribers and account holders of the service provider's system or internet of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or internet who are repeat infringers."[404] After examining this

403 E-commerce Directive (n1), Recital 45.

404 DMCA (n1), Sec. 512 (i) (1) (A).

provision, its focus is on infringing users rather than on infringing content, which can be properly called a repeat infringer policy, and ISPs' clients must also be informed about this policy.

The repeat infringer policy is closely related to the DMCA "notice-take down" mechanism. First, only after a qualified notification has been sent, which is sufficient for the hosting ISP to locate the infringing content, will the court investigate whether the hosting ISP has implemented a policy against repeat infringing properly. For example, in the case of *Perfect 10, Inc. v. CCBill, LLC*, the notice sent by Perfect 10 only identified the website that contained the alleged infringing materials, but did not identify the URLs of the images nor identify which of its images were being infringed, so the notice failed to provide IBill with enough information to locate the infringing materials.[405] Therefore, the court found that this notice could not support the claim that IBill had failed to reasonably implement its repeat infringer policy.[406] Second, a hosting ISP must name a proper agent to receive notifications of complaint. In *Ellison v. Robertson*, the defendant had changed the e-mail address to which "the infringement notifications were supposed to have been sent", and "failed to provide for the forwarding of messages sent to the old address or notification that the e-mail address was inactive", so the court found that the defendant did not have an effective notification agent in place at the time when the alleged infringing activities had occurred, and thus had not reasonably implemented its policy against repeat infringers.[407] Third, unlike the notice-take down procedure, notices of copyright infringement from a non-party are relevant in deciding whether the repeat infringer policy is properly implemented. In the case of *Perfect 10, Inc. v. CCBill, LLC* , the appeals court held that § 512(i)(1)(A) required it to assess the service provider's "policy" rather than how the service provider actually treated a particular copyright owner, so defendants' actions towards non-parties were relevant in determining whether defendants had reasonably implemented their repeat infringer policy.[408]

Since there is a public policy against repeat infringers, it is important to define and discuss what "repeat" should mean in the context of infringement. However, it seems that the US courts did not exert much effort in interpreting the concept of repeat infringer. In the case of *Perfect 10, Inc. v. CCBill, LLC*, the court found that both of the following circumstances conform to repeat infringer policy: 1) upon receiving notice from the plaintiff that complied with the DMCA's notification requirements, defendant - IBill had suspended the offending web site's account;[409] 2) the defendant's Internet Key would ban a webmaster from its age-verification

405 See *Perfect 10, Inc. v. CCBill, LLC* (n268), at 1090. This opinion has been upheld by 9th Circuit Court in the appealing instance; see *Perfect 10, Inc. v. CCBill LLC* (n336), at 1113.

406 Ibid.

407 See *Ellison v. Robertson*, 357 F3d 1072, at 1080 (9th Cir, 2004).

408 See *Perfect 10, Inc. v. CCBill LLC* (n336), at 1113.

409 See *Perfect 10, Inc. v. CCBill, LLC* (n268), at 1090.

service after it had received three notifications regarding the web sites of any particular webmaster.[410] Therefore, at least in the U.S. District Court for the Central District of California, it is tolerable if an ISP does not enforce its repeat infringer policy against an internet user after its second infringement. Additionally, it is worth noting that Congress requires reasonable implementation rather than perfect implementation.[411] Hence, although an ISP's policy can be easily sidestepped by infringing internet users, such as opening a new account after their original accounts have been terminated, the efforts to sidestep the defendant's policy do not amount to a failure of implementation on the part of the defendant.[412] Moreover, to identify and terminate the accounts of repeat infringers, the ISPs also do not need to track users in a particular way to or affirmatively police users for evidence of repeat infringement.[413] However, impeding the proper implementation of this policy is prohibited. In the case of *Aimster*, an encryption system was built into the defendant's system which prevented it from knowing which users were transmitting which particular file, so actually the repeat infringer policy could never be implemented, and based on this the court concluded that the defendant failed to satisfy the threshold requirement of DMCA 512 (i)(A).[414] Nevertheless, if a hosting ISP does not allow the copyright owner to take advantage of the content-identification tool that is only open to its partners, the hosting ISP may not violate the repeat infringer policy. In the case of *Viacom v. YouTube*, the defendant YouTube adopted the content identification tools which allowed the copyright owners who had partnership with it to identify their copyrighted materials on YouTube, but Viacom was not a partner of YouTube and thus could not utilize the content identification tools.[415] Therefore, Viacom claimed that YouTube "deliberately set up its identification tools to try to avoid identifying infringements of class plaintiffs' works," and thus violated the repeat infringer policy.[416] The court first defined the deployment of the content identification tools as a sort of monitoring measure taken by YouTube, and then referred to DMCA 512(m)(1) which reads that "a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i)."[417] Then, the court held that only "refusing to accommodate or implement a 'standard technical measure' exposes a service provider to liability," but "refusing to provide access to mechanisms by which a service provider affirmatively

410 Ibid, at 1093.
411 Ibid, at 1089.
412 *Corbis Corp. v. Amazon.com, Inc.* (n333), at 1103. See also *Io Group, Inc. v. Veoh Internets, Inc.* (n5), at 1143-1145.
413 Ibid.
414 *In re Aimster Copyright Litigation* (n66), at 655.
415 *Viacom International, INC. v. YouTube, INC.* (n7), at 41.
416 Ibid.
417 Ibid.

monitors its own network has no such result."[418] Since the content identification tools in question were not the standard technical measure prescribed in DMCA 512 (i), YouTube should not be excluded from safe harbor for restricting access to the content identification tools.[419] In fact, content identification tools deployed by YouTube function as a convenient way for its partners to identify their copyrighted materials, but the non-partner copyright owners still can use normal measures to identify their contents on YouTube, so the content identification tools in this case are substantially different from the encryption system deployed by Aimster.

4.3.2 Repeat Infringement in the EU

At the EU level, the relevant Directives confer upon copyright owners the right to apply for an injunction against ISPs whose services are used for copyright infringement. For instance, the Article 8(3) of Information Society Directive provides that "Member States shall ensure that rights holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right."[420] But the Directive does not include any condition and modality relating to such injunctions, and leaves the details of injunction rules to the national law of the member states.[421] Meanwhile, the IP Enforcement Directive reconfirms these injunction rules provided in the Information Society Directive.[422] Further, in the light of this Directive, all remedies including injunctions "shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays," and "shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse."[423]

In the case of *L'oreal v. eBay*, the ECJ also held that Member States had the right to order the hosting ISP concerned to take measures that not only bring to an end the infringement of a copyright or trademark holder's rights, but also prevent further infringement.[424] Regarding the measures that can be ordered in an injunction, the ECJ further stated that, the measures should not conflict with "no general monitoring obligation" clause,[425] and "must be effective, proportionate, dissuasive," and "must not create barriers to legitimate trade."[426] However, except providing these three general criteria, the ECJ did not indicate any explicit measure that can be ordered in an injunction, and left it for national courts to decide at their discretion.

418 Ibid.
419 Ibid.
420 Directive 2001/29/EC (n83), Art. 8(3).
421 Ibid, Recital 59.
422 Directive 2004/48/EC (n83), Art. 11.
423 Ibid, Art. 3.
424 *L'Oréal SA and Others v eBay International AG and Others* (n327), at para. 125-134.
425 Ibid, para. 139.
426 Ibid, para. 144.

Therefore, in the EU, copyright owners can apply for injunctions from courts so as to require hosting ISPs to prevent infringement from occurring in the future. Nevertheless, whether hosting ISPs are obligated to, or to what extent hosting ISPs should take measures to prevent repeat infringement in the future, mainly depends on the national law in the member states. In fact, because the same infringing materials can easily be uploaded again after being taken down, in order to effectively prevent such endless notice-and-takedown process, the courts in member states do request hosting ISPs to take necessary measures against repeated infringement. The following section explores how national courts define hosting ISPs' obligations against repeating infringement under the roof of the EU Directives.

4.3.2.1 Störerhaftung - Disturber's Liability in Germany

As discussed in the section about "hosting ISPs' knowledge in Germany", a hosting ISPs' knowledge of infringement is difficult to prove without proper notification from the copyright owners, so liability based on knowledge can rarely be found by a court. However, German law offers an alternative basis on which to impose hosting ISPs' liability, störerhaftung, which can be translated as "disturber's liability" in English. According to Article 97 of German Copyright law (UrhG § 97),

> Any person who infringes copyright or any other right protected under this Act may be required by the injured party to eliminate the infringement or, where there is a risk of repeated infringement, may be required by the injured party to cease and desist. Entitlement to prohibit the infringer from future infringement shall also exist where the risk of infringement exists for the first time.[427] 107

"Disturber's liability" is a kind of liability which requires the responsible party to prevent certain infringements from occurring again in the future. The TMG § 10 only limits the monetary damages liability of qualified hosting ISPs, but the other remedies such as "disturber's liability", can remain unaffected by TMG § 10. Currently, whether the hosting ISPs should face "disturber's liability" has become a main point of contention by parties before the German Courts. Prof. Leistner notes that if someone runs an automatic processing system (such as a platform automatically processing the contents uploaded by its users), it is not practical for him to acquire the knowledge or control over the information transmitted in the system; however, in order to ensure it is free of liability in this way, it must adapt itself in the future to qualify for the following requirement, namely, based on the intensified duties established in the context of "disturber's liability", it should at least take minimal control over the transmitted information after receiving clear notices about concrete infringements.[428]

427 German Copyright Act, Sec. 97 (1).

428 Leistner M, 'Grundlagen und Perspektiven der Haftung für Urheberrechtsverletzungen im Internet', 2012 ZUM

The German Federal Court of Justice made a fundamental and proper development of the breadth of "disturber's liability" for the hosting ISPs. Upon receiving evidence about a concrete and obvious infringement, the relevant ISP should not only block this concrete infringement; but it is also responsible for taking all possible and reasonable measures to prevent substantially similar infringements from occurring in the future.[429] As for what constitutes possible and reasonable measures, the German courts have different opinions. In Sharehoster II, the Higher Regional Court of Hamburg followed a strict approach to an ISP's monitoring duty, and required the defendant, after being notified by the plaintiff of a particular infringement, to undertake a preventive search (both automatic and manual) of all hosted content in order to identify the material infringing the plaintiff's rights, and check all the files uploaded by users who have previously uploaded infringing content.[430] The Higher Regional Court of Düsseldorf, by contrast, seems to have favored the hosting provider, and found that the measures applied by the ISP (essentially the same as those in the case before the Hamburg Court) were sufficient, but the monitoring duties required by the plaintiff, such as word filtering of titles, manual searching and blocking IP addresses, were unreasonable.[431]

Moreover, academics in Germany are also enthusiastic about setting a proper criterion for "disturber's liability". In Prof. Leistner's opinion, because of
108 E-Commerce Directive Article 15 (§ 7 Abs. 2 TMG), no general active monitoring responsibility should be taken into account. In any case, if legal business-models are worthy of protection, they are usually only obliged to take economically reasonable filtering conduct (usually only automatic measures are feasible).[432] However, when analyzing the ISP's legal business-model it is still necessary to distinguish between dangerous and neutral business-models. The former means a business-model which could easily result in infringements based on its previous advertising, design, and the funding structure of its platform, while the latter means a business-model which is not particularly friendly to infringements due to its marketing, structure of platform, and benefiting model.[433] For the active disturber (the one who runs the dangerous model), if it still operates a legal business-model, then the further control and duties are not unreasonable so as to make the particular dangerously structured business-model neutral again.[434] From the above-statement, the hosting

731.

429 Ibid, at 724.

430 Sharehoster II, 2010 MMR 51, at 53 (quoting Matulionyte and Nérisson, 'The French Route to an ISP Safe Harbor, Compared to German and US Ways' (n231), at 66)

431 Rapidshare, 2010 MMR 483, at 484 (quoting Matulionyte and Nérisson, 'The French Route to an ISP Safe Harbor, Compared to German and US Ways' (n231), at 66-67)

432 Leistner, 'Grundlagen und Perspektiven der Haftung für Urheberrechtsverletzungen im Internet' (n423), at 725.

433 Ibid.

434 Ibid.

ISPs' intent, which can be deduced from its business-model, is an important factor when deciding how broad the "disturber's liability" should be, which means that if a hosting ISP has the intent to promote the infringing use of its platform, it is reasonable to ask it to take more responsibility in the frame of "disturber's liability". In the case of "*Rapidshare*", the German Federal Court of Justice also delivered a similar opinion. It concluded that when deciding the scope of responsibilities as a disturber, the following two factors should be considered: (1) whether the business-model of a hosting ISP is designed for infringements from the beginning or not, and (2) whether it promotes the infringing use of its service by its own measures.[435] If a hosting ISP induces copyright infringements committed on a substantial scale, it is reasonable for it to take comprehensive and regular control over the "links collections"[436] which refer to its service.[437]

To conclude, unlike the repeat infringer policy in the US, in Germany substantial measures are required to be taken against repeat infringement of the same content rather than repeat infringers. However, similarly to the US, these measures taken by hosting ISPs should be possible and reasonable, but they do not need to be perfect. As for what the possible and reasonable measures are, that depends on the hosting ISPs' intent as mirrored in their business-model. This means that the more likely a hosting ISP's business-model is to result in infringements, then more sophisticated measures against repeat infringement of content are possible and reasonable. In addition, the enforcement of disturber's liability in Germany is also relevant to the notice-and-takedown procedure, because generally a proper notification from the copyright owner needs to be sent so as to trigger disturber's liability.

4.3.2.2 Stay-down in France

In the EU, in order to prevent the same infringing materials from being repeatedly uploaded, the courts in Member States developed a "notice and stay-down" mechanism by case law.[438] In the light of "notice and stay-down" mechanism, a hosting ISP is obligated to take necessary and permanent measures to prevent the infringing materials, which had been the subject of complaint in notices, from being uploaded on its platform again.[439] Since 2007, some French courts have already introduced the "notice and stay-down" mechanism, required the hosting ISPs to take all necessary measures to monitor the materials which had been notified

435 BGH – *Rapidshare* (n42), Para. (b).

436 "link collections" means the collections of search results after searching for specific content through search tools. For instance, if a person searches keywords of "alone in dark, Rapidshare" in Google, the results are links from which a person can download "alone in dark" residing on Rapidshare.

437 BGH – *Rapidshare* (n42), Para (c).

438 Parti K and Marin L, 'Ensuring freedoms and protecting rights in the governance of the Internet: a comparative analysis of blocking measures of illegal Internet content and the liability of ISPs' (2013) 9 Journal of Contemporary European Research 138, at 149.

439 Ibid.

as illegal.[440] For instance, in Tranquility Bay the TGI de Paris (High Court of Paris) concluded that, once the defendant had been notified about the infringing materials, it was obligated to implement any possible means to prevent the same infringing materials from being uploaded again; otherwise, it could not be sheltered under safe harbor protection. [441] In 2011, the Paris Court of Appeal held Google Video liable because it failed to take every possible means to prevent the complaint videos in copyright owner's notifications from being accessed again.[442] However, after the ECJ reaffirmed the doctrine of "no general monitoring obligation" in the case of *Scarlet Extended SA v. SABAM*, the "notice and stay-down" mechanism was dismissed by French courts.[443] In 2012, the Cour de Cassation (Supreme Court) put an end to this "notice and stay-down" mechanism based on the reason that this mechanism cannot be achieved without undertaking a general monitoring obligation.[444] According to the reasoning made by the court, although it seems only to impose a specific monitoring liability on Google by requiring it to prevent the same infringing content from being accessed again, it is impossible to find this repeat infringing content without screening all posted content (including non-infringing ones), which amounts to subjecting Google to a general obligation to monitor.[445] As noted by Angelopoulos Christina, since the materials specified by the notifications can accumulate at a really fast speed, the only way to monitor such a large amount of "specified" materials is to use fingerprinting or similar automatic filtering technologies to check every upload.[446]

4.3.2.3 Stay-down in Italy

In Italy, in order to prevent the endless take-down and reposting process, copyright owners tend to request the courts to order hosting ISPs to prevent the same infringing materials from being uploaded again. However, such a kind of claim cannot always be confirmed by courts. For instance, in the case of *RTI v. Google*, some football match videos copyrighted by RTI were embedded and linked on a blog hosted by Google's Blogger.com, so it requested Google to remove the infringing materials and

440 Angelopoulos, 'Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe' (n91), at 264.

441 Ibid.

442 Ibid.

443 Parti and Marin, 'Ensuring freedoms and protecting rights in the governance of the Internet: a comparative analysis of blocking measures of illegal Internet content and the liability of ISPs' (n433), at 149. In the case of Scarlet Extended SA v SABAM, the European Court of Justice stated, that Member States must not put ISPs under any obligation to endorse illegal police activities and thus providing surveillance of users. The ECJ also ruled that national court's order to force ISPs to implement filter systems, installed at ISPs' own expense and used for an unlimited period of time, would breach the ISP's rights to conduct business freely, and would infringe individuals' rights to privacy and personal data protection.

444 Angelopoulos, 'Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe' (n91), at 265.

445 Ibid.

446 Ibid.

prevent them from being posted again.[447] The District Court of Rome held that the plaintiff's claim conflicted with no general monitoring Clause in the E-commerce Directive, and Google had no obligation to filter out the infringement in the future.[448] It is commonly believed that the District of Rome was affected by the ECJ case "Scarlet Extended SA v SABAM", when making this decision.[449] However, in the case of *Delta TV v. YouTube*, the District Court of Turin to some extent took a different decision. In this case, some of videos copyrighted by Delta TV were uploaded on YouTube without permission, so the Delta TV sent some complaint notices to YouTube, and requested YouTube to take the necessary measures to prevent the infringing materials indicated in the notices from being uploaded again.[450] In the decision, besides deciding the necessary elements of a competent notice which can provoke the hosting ISPs' responsibility to remove the materials in question, the District Court of Turin also held that YouTube should allow the Delta TV to use the Content ID system[451] to prevent the same infringement from being committed again.[452] According to the Content ID policy made by YouTube, copyright owners should submit the reference files used for filtering by themselves at their own cost.[453] But the District Court of Turin held that after receiving a competent notice, YouTube is obligated to incorporate the infringing materials into the Content ID system as reference files at its own cost so that the Content ID system can filter out the further infringement.[454] In the decision, the District Court of Turin also referred to the ECJ case "Scarlet Extended SA v SABAM", and reconfirmed that ISPs should not be requested to actively monitor the materials uploaded by users, and then held that it was not active monitoring to keep the infringing materials stay-down by relying on Content ID.[455] Therefore, with the development of filtering technologies, the Italian courts seem to also update their views on stay-down obligation.

447 Decision of the Court of Rome of July 11, 2011, quoting Coraggio G, 'Google's victory might be a short success' (2012) 23 Entertainment Law Review 139, at 140.

448 Ibid.

449 Ibid. In the case of *Scarlet Extended SA v SABAM*, the ECJ held that "must be interpreted as precluding an injunction made against an internet service provider which requires it to install a system for filtering … which is capable of identifying on that provider's network the movement of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold intellectual-property rights, with a view to blocking the transfer of files the sharing of which infringes copyright." See *Scarlet Extended SA v SABAM* (n70).

450 Coraggio G, *YouTube case changes rules on Internet liability*, Lexology(2014), *available at* http://www.lexology.com/library/detail.aspx?g=bf912a7f-b3d2-47b2-9fed-c50534122b00 (last visited 26-04-2014).

451 Content ID is an anti-piracy system run by YouTube and it can be used to filter out the copyrighted materials by reference files, see How Content ID works (n42).

452 Spedicato G, *Italy: the take-down notice must contain the specific YouTube URLs*, Wolters Kluwer(2014), *available at* http://kluwercopyrightblog.com/2014/05/28/italy-the-take-down-notice-must-contain-the-specific-youtube-urls/ (last visited 27-08-2014).

453 How Content ID works (n42).

454 Coraggio, YouTube case changes rules on Internet liability (n445).

455 Ibid.

4.3.2.4 Injunction in the UK

In the UK, the injunction provision in Information Society Directive was implemented by Sec. 97A of the Copyright, Design and Patent Act, which reads that "the High Court (in Scotland, the Court of Session) shall have power to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright."[456] When determining whether an ISP has the actual knowledge in this section, "a court shall take into account all matters which appear to it in the particular circumstance to be relevant," and particularly, whether the ISP has received a competent notice.[457] Therefore, after notifying a hosting ISP about copyright infringement, the copyright owner can apply for an injunction order against the hosting ISP, and prevent it from offering its service to the infringing party. Nevertheless, such a notice should not be held a pre-condition to conclude that a hosting ISP acquires actual knowledge of other parties infringing copyright through its service.[458] Regarding the breadth of injunction, the UK courts refer to the injunction rules at the EU level, and hold that an ISP may not only be required to prevent the continuation and repetition of the infringement that it has actual knowledge of, but also prevent the "further infringement of that kind".[459] Nevertheless, when deciding the scope of injunction in a concrete case, the court should ensure that the injunction entitled to copyright
112 owner must be dissuasive, effective and proportionate, and must not hamper the legal business.[460] Further, a copyright owner is only authorized to seek an injunction to restrain the illegal transmission of its own copyrighted works. In the case of *Twentieth Century Fox Film Corp v. Newzbin Ltd*, the plaintiffs tried to seek an injunction that covers all binary and all text materials including those they did not have rights to, but eventually, the court held that this injunction request was unreasonable, and only granted the plaintiffs an injunction to "restrain the defendant from infringing claimants' copyright in relation to their repertoire of films."[461]

To sum up, compared with the repeat infringer policy in the US, the hosting ISPs in the EU are required to take measures against repeat infringement of the same materials rather than against repeat infringers. However, it is still questionable whether such obligation of preventing the same infringing materials from being

456 UK Copyright, Designs and Patents Act 1988 (n128), Sec. 97A(1).

457 Ibid, Sec. 97A(2).

458 *Twentieth Century Fox Film Corp v Newzbin Ltd*, [2010] EWHC 608 (Ch), Para. 134, 135. In this case, although the defendant denied that it had actual knowledge of any person using its service to infringe, because it did not receive any notice from the plaintiff, the court still held that the defendant acquired the actual knowledge prescribed in Section 97A.

459 *Twentieth Century Fox Film Corp v. British Telecommunications Plc*, Royal Courts of Justice, [2011] EWHC 1981 (Ch). Para. 153-156.

460 Ibid.

461 *Twentieth Century Fox Film Corp v. Newzbin Ltd* (n453), Para. 135.

uploaded complies with the "no general monitoring obligation" clause in the E-Commerce Directive. For example, the French courts have adopted the "notice and stay-down" mechanism, but in 2012, the French Supreme Court dismissed this mechanism, since it was inconsistent with the "no general monitoring obligation" clause.[462] In Italy, the courts seem to adopt a compromising approach. Although they recognize that stay-down obligation may conflict with "no general monitoring obligation" clause, they hold that copyright owners should be allowed to use the anti-piracy tools that have been deployed by hosting ISPs to keep the infringing materials stay down.[463] In Germany, based on the disturber's liability in Tort Law, German courts require a hosting ISP not only to remove the infringing materials in question after receiving complaining notices, but also to take all necessary and reasonable to prevent the same infringing materials from being uploaded again.[464] In order to avoid conflicting with "no general monitoring obligation" clause, the obligations under disturber's liability is named as specific monitoring.[465] In the UK, an injunction can be ordered against the hosting ISP which has actual knowledge of infringement, and it can require the hosting ISP to prevent the continuation and repetition of that infringement, or even stop the further infringement of that kind.

4.3.3 Repeat Infringement from the Same Internet User in China

Although the Internet Regulation adopts the "notice-and-takedown" mechanism, it does not include a provision requiring ISPs to take action against repeat infringers or the repeat infringement of the same content. However, the General Principles of the Civil Law of the People's Republic of China, as a fundamental legal document protecting private rights, provides a general liability rule which is quite similar to the "disturber's liability" in German civil law as follows: 1) cessation of infringements; 2) removal of obstacles; 3) elimination of dangers.[466] Based on the rationale embodied in the Chinese "disturber's liability", some courts require hosting ISPs to take essential measures against repeat infringements. For instance, in the case of *Yinian v. Taobao*, although the defendant Taobao had already deleted the infringing

462 Angelopoulos, 'Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe' (n91), at 265.

463 Coraggio, YouTube case changes rules on Internet liability (n445).

464 M. Leistner, 'Grundlagen und Perspektiven der Haftung für Urheberrechtsverletzungen im Internet', (n423), at 725.

465 Matulionyte and Nérisson, 'The French Route to an ISP Safe Harbor, Compared to German and US Ways' (n231), at 66.

466 National People's Congress (全国人民代表大会), General Principles of the Civil Law of the People's Republic of China (中华人民共和国民法通则), Order No. 37 of the president of the People's Republic of China (中华人民共和国第37号主席令), Art. 134. The legislators in China used Art. 1004 of German Civil Law as an important reference, which provides that "If the ownership is interfered with by means other than removal or retention of possession, the owner may require the disturber to remove the interference. If further interferences are to be feared, the owner may seek a prohibitory injunction", when drafting Art. 134. This kind of "störerhaftung" has also been reaffirmed by the newly-adopted China Tort Law in Art. 15.

content after receiving complaints which all pointed to one account (the owner of this account was another defendant in this case), this account still existed even after seven complaints. Based on this fact, the Court then concluded that the defendant had not fulfilled its duty of care, so it faced contributory liability.[467] In the case of *Han Han v. Baidu*,[468] the plaintiff sent notification complaining that one of his books "Xiang" had been uploaded onto the defendant's literature-sharing platform without permission.[469] After receiving notice, the defendant deleted the infringing content; however, the same infringing content under a different title could still be accessed on the defendant's platform.[470] Based on these facts, the Court concluded that the defendant had not taken sufficient measures to prevent the infringing content from being transmitted through its platform, despite the fact that the defendant claimed it had run an anti-piracy system.[471]

By comparing the two cases cited above, it appears that that, according to the first case, courts that require the hosting ISPs to terminate accounts repeatedly used for infringing activities, are likely to adopt the US approach. In contrast, by deducing from the second case, courts requiring the hosting ISPs to prevent the same infringing content from being accessed again are more likely to follow the stay-down (EU) approach. This difference shown in these two cases, demonstrates that the Chinese courts know of the necessity of requiring hosting ISPs to prevent repeat infringements, but they are not entirely sure which approach to adopt. This struggle is also reflected in the newly issued Internet Provision. In the draft of the Internet Provision, it stated that the ISP should take reasonable measures to prevent the infringement of the same content from occurring again, which is typical of the stay-down approach.[472] However, the final version of Internet Provision includes a more nuanced expression: whether the ISPs take reasonable measures against repeat infringements made by the same internet user.[473] This can be understood in two ways: first, if "repeat" is interpreted as "same", namely, the same infringements made by the same internet user, it is a "double requirement of identity" standard such as that advocated by the EU Advocate General in the case of "*L'Oréal SA*

467 *Yinian v. Taobao (衣念v.淘宝)*, Shanghai First Intermediate People's Court (上海市第一中级人民法院), No. 40 Hu Yi Zhong Min Wu (Zhi) Zhong Zi (2011) (（2011）沪一中民五（知）终字第40号). This case was published in the Bulletin of People's Supreme Court (Vol. 1, 2012) as a guiding case.

468 Han Han is one of most distinguished young writers who has many fans in China, and in May 2010, he was named one of most influential people in the world by Time magazine. The other party, Baidu, can be seen as the Chinese Google, and is one of the most successful internet companies in China. Therefore, the dispute between these two parties attracted considerable attention and, finally, this case was selected as one of ten annual IP cases (2012) by the People's Supreme Court.

469 *Han Han v. Baidu (韩寒v.百度)* (n42).

470 Ibid.

471 Ibid.

472 Internet Provisions (n208) (Draft) (网络规定(草案)), Art. 8 (6).

473 See Internet Provisions (网络规定) (n208), Art. 9 (6).

v. eBay";[474] second, if "repeat infringement" is understood more broadly, meaning all infringements after the first one made by the same internet user count as repeat infringements, then it looks more like a rule against repeat infringers, because terminating the repeat infringer's account seems the only efficient way of getting rid of these repeat infringements. As for what constitute reasonable measures, in the case of "*Han Han v. Baidu*", the court held that manual monitoring measures should not be imposed, because they are too burdensome to be continuous; regarding technical measures, whether they are reasonable depends on the current technical level and will change with the development of new technologies.[475] Furthermore, the court held that the measures need not be perfect and that the following measure is inappropriate, namely, using the author's name plus the title of the work as keywords to filter out infringing content, because that in turn might block considerable legal content.[476]

By comparing the rules against repeat infringement in the US, EU and China, it appears that the US rules focus on punishing repeat infringers, the EU rules focus more on preventing the repeat infringement of content, and the rules in China can be understood as a mixed solution, which not only ask hosting ISPs to prevent the repeated infringing of content based on the "double requirement of identity" (a limited EU approach), but also require hosting ISPs to terminate the accounts of repeat infringers (a US approach). Of these three approaches, the EU one imposes the heaviest burden on hosting ISPs, because hosting ISPs need to monitor these infringing materials so as to prevent them from being uploaded on the platforms again. By contrast, the Chinese approach only requires hosting ISPs to prevent the same user from uploading the same infringing materials. Regarding terminating the accounts of repeat infringers, it can be fulfilled without complicated monitoring efforts, and although the policy of terminating accounts can easily be sidestepped by creating new accounts, hosting ISPs do not need to be responsible for the sidestepping done by Internet users. To be mentioned, although in the US hosting ISPs are not obligated to prevent the same infringing materials from being uploaded again, the US courts hold such efforts as evidence to prove the hosting ISPs' due diligence in preventing infringement. For instance, Veoh, a video-sharing website in the US, has adopted means for generating a "hash", or digital "fingerprint", for each video, which essentially enables Veoh to terminate access to any other identical files and prevent

474 Opinion of Advocate General, C-324/09 (n291), Para. 182. In this case, the AG first admitted that nothing in Directive 2004/48 would prohibit injunctions against the intermediary requiring not only the prevention of the continuation of a specific act of infringement but also the prevention of repetition of the same or a similar infringement in the future if such injunctions are available under national law. However, he also emphasized legal certainty and that an injunction should not impose impossible, disproportionate or illegal duties such as a general obligation to monitor. He concluded that an appropriate limit for the scope of injunctions may be that of a double requirement of identity.

475 See *Han Han v. Baidu (韩寒v.百度)* (n42).

476 Ibid.

additional identical files from ever being uploaded by any user.[477] The court took Veoh's efforts against repeat infringement as one reason to conclude Veoh fulfilled its duty of care and thus should be exempted from liability.[478] Further, in order to prove their diligence against copyright infringement in front of courts, some Chinese hosting ISPs also implement technologies to filter out the infringing materials which are repeatedly uploaded. For example, Tudou, a video-sharing website, has established a database called "collection of black content", and any video which has been complained about will be marked with a fingerprint and put into the database for comparison with videos uploaded thereafter, so as to filter out repeat infringing content.[479] Finally, in all three jurisdictions a common restriction has been set on required measures, and that is that the measures only need to be "reasonable" rather than "perfect".

4.4 Benefit from Infringements

In the US common law, directly benefiting from infringements is one of two prongs for concluding vicarious liability, and the other is having the right and ability to control the infringements.[480] The US "safe harbor" provision also adopts a similar rule to regulate hosting ISPs' secondary liability.[481] By contrast, in the EU and China where vicarious liability does not apply, benefiting or profiting from infringements is not an independent culpable element when concluding liability in the copyright field. However, when hearing cases about hosting ISPs' secondary liability, the courts in the EU and China still take into account the hosting ISP's benefit or intent to benefit.

116

4.4.1 Direct Benefit in US

According to DMCA §512(c)(1)(B), in the US, if a hosting ISP wants to be exempted from secondary liability, "it should not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity". In a literal sense, the substantial contents of this provision are quite similar to the vicarious liability rule in US common law.

477 See *Io Group, Inc. v. Veoh Internets, Inc.* (n5), at 1143.

478 Ibid.

479 During a workshop about "video-sharing website's secondary liability" held in the Center for Studies of Intellectual Property Rights of Zhongnan University of Economics and Law, the former legal director, Mr. Guangliang Cai delivered an introduction about the anti-piracy measures adopted by Tudou, which covered the database of black content. The relevant statement can also be found in Tudou's copyright policy from its website, see http://www.tudou.com/about/cn/copyright.html.

480 See *Gershwin Publishing Corp. v. Columbia Artists Mgmt., Inc.* (n76), at 1162.

481 See DMCA (n1), Sec. 512 (c)(1)(B). According to this Article, if a hosting ISP wants to be exempted from secondary liability, it should not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity.

However, the Congressional report specifically states that: the liability limitation provided in DMCA 512 "protects qualifying service providers from liability for all monetary relief for direct, vicarious and contributory infringement."[482] Therefore, it seems that the "financial benefit" and "right and ability to control" in DMCA 512 (c)(1)(B) may be interpreted differently from the same terms in the context of an allegation of vicarious liability. However, not all US courts follow the indication in the Congressional report. For example, in *Costar Group Inc. v. Loopnet, Inc.*, Judge Chasanow concluded that: "the DMCA provides no safe harbor for vicarious infringement because it codified both elements of vicarious liability".[483] In *Perfect 10, Inc v. CCBill LLC*, the Ninth Circuit held that 'direct financial benefit' should be interpreted consistently with the similarly-worded common law standard for vicarious copyright liability."[484] However, for most US courts, the statement in the legislative history seems a more reasonable interpretation and persuasive. For instance, in the appeal of *Costar Group Inc. v. Loopnet, Inc.*, the Fourth Circuit held that even though an ISP should undertake vicarious liability under common law, it "may still look to DMCA for safe harbor if it fulfilled conditions therein."[485] In a case closed in 2012, the Ninth Circuit also concluded that in some cases ISPs subject to vicarious liability can be exempted from monetary remedies if they fulfill the requirements of the "safe harbor" provision, and specified that the "right and ability to control such activity" in DMCA 512 (c)(1)(B) should be interpreted more narrowly than analogous terms under vicarious liability.[486]

As for what is the direct benefit in DMCA §512(c)(1)(B), according to the House Report, if an ISP principally runs a legal business and charges infringers the same fees as it charges non-infringing users, then the profit received by the ISP is not directly attributable to infringements.[487] Therefore, "receiving a one-time set-up fee and flat, periodic payments for service" from an infringer would not constitute direct benefits, nor would receiving fees "based on the length of the message or by connect time". However, "where the value of the service lies in providing access to infringing materials", the foresaid fees should be accounted as direct benefit.[488] In case law, besides referring to the Report above,[489] the US courts also rely heavily on the standard about benefiting directly as developed under the vicarious liability in

482 Congress, U.S., House Report 105-796 (1997-1998) (thereafter H.R. Conf. Rep. No. 105-796), at 73.

483 Costar Group Inc. v. Loopnet, Inc., 164 F. Supp. 2d 688, at 704 (D. Md. 2001).

484 See *Perfect 10, Inc. v. CCBill LLC* (n336), at 1117.

485 *Costar Group Inc. v. Loopnet*, Inc. (n263), at 555.

486 See *UMG Recording, Inc. V. Veoh Internet, Inc.* (n291), at 1042-1045. In this case, the plaintiff UMG is a recording company which has copyright over considerable amounts of music, some of which was uploaded onto the defendant's running video-website Veoh, so the plaintiff sued Veoh for copyright infringement.

487 See H.R. REP. 105-551(II) (n16), at 54.

488 Ibid.

489 See *Costar Group Inc. v. Loopnet, Inc.* (n478), at 720. In this case, the court held that it would not be considered as a direct financial benefit "where the infringer makes the same kind of payment as non-infringing users of the provider's service".

common law, and thus base their conclusion on "whether the infringing activity constitutes a draw for subscribers, not just adding benefit".[490] Regardless of whether they follow the criteria stated in the House Report or the "constituting a draw" standard in common law, it is held that the defendant's hosting of websites for a fee was not sufficient to prove its receiving direct financial benefit from infringements.[491] However, charging fees based on offering a host service is only one way of making profits, and nowadays it is quite typical for a hosting ISP to offer a free hosting service, but sell advertising space to generate profits, as Veoh, YouTube, and other content-sharing websites do. This raises the question, therefore, of whether the sale of advertising space can be identified as making a direct financial benefit from infringements. The US courts seem to avoid answering this question, but instead try to resolve the problem of hosting ISPs' qualifying for DMCA 512 (c)(1)(B) by analyzing whether the hosting ISPs have the right and ability to control the infringements. This is because if a hosting ISP has no right and ability to control the infringements, then the court does not need to consider whether the hosting ISP receives direct benefit from infringements, and thus it certainly qualifies for DMCA 512 (c)(1)(B). For instance, in the case of *Io v. Veoh*, the Court held that "even assuming (without deciding) that Veoh received a direct financial benefit from the alleged infringing activity," since the "defendant does not have the right and ability to control such activity," the defendant still did not lose its qualification for DMCA 512 (c)(1)(B).[492] In the first instance of *Viacom v. Youtube*, the Court admitted that "there may be arguments whether revenues from advertising, applied equally to space regardless of whether its contents are or are not infringing, are 'directly attributable to' infringements," but then based on YouTube's lack of right and ability to control the infringements, it then held that YouTube still qualified for the DMCA 512 (c)(1)(B) safe harbor.[493]

118

490 See *Perfect 10, Inc. v. CCBill LLC* (n336), at 1117; see *Io Group, Inc. v. Veoh Internets, Inc.* (n5), at 1150. This standard can be traced to the classic case of *Fonovisa v. Cherry Auction* (76 F.3d 259, at 264 (9th cir. 1996)). In this case, the Ninth Circuit held that the sale of pirate recordings in a Cherry Auction swap meet is a "draw" for customers, so the defendant who ran this swap meet directly benefited from infringements.

491 Ibid, Perfect 10, Inc. v. CCBill LLC (n336), at 1118. In this case, the defendant, CWIE, hosted websites for a fee, and some of these websites included content which infringed the plaintiff's copyright. First, the Ninth Circuit held that the defendant's hosting of websites for a fee was not sufficient to prove the infringements functioning as a "draw" in the context of vicarious liability. Further, by noting that " receiving a one-time set-up fee and flat, periodic payments for service from a person engaging in infringing activities would not constitute receiving a 'financial benefit directly attributable to the infringing activity'", the Ninth Circuit held that the hosting fee received by the defendant was not directly attributable to infringements.

492 *Io Group, Inc. v. Veoh Internets, Inc.* (n5), at 1150.

493 See *Viacom International, INC. v. YouTube, INC.* (n2), at 517. In this case, the court held that in any event the provider must know of the particular case before he could control it. This interpretation of "control" has been overruled by the appeal court, which specified that "control" has nothing to do with hosting ISPs' "item-specific" knowledge of infringements. See *Viacom International, INC. v. YouTube, INC.* (n7), at 36-38.

When it comes to having the "right and ability to control infringement", nearly all US courts[494] have held that the control provision in the DMCA 512 (c)(1)(B) should be interpreted differently from the common law vicarious liability criteria, and that it "required something more than the ability to remove or block access to materials posted on a service provider's website".[495] The "something more" standard was derived from the "notice-and-takedown" procedure in the DMCA, because in order to conform to the "notice-and-takedown" procedure, a hosting ISP must have the right and ability to remove or block the infringement complained of by the copyright owner.[496] Regarding what constitutes "something more", only a few US courts have made relevant statements. In *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, which is the only case to conclude that an ISP has the right and ability to control infringement under the DMCA §512(c)(1)(B),[497] the court based its conclusion on the following facts: the defendant ran a monitoring program to notify service receivers with "detailed instructions regarding issues of layout, appearance, and content", and if a service receiver failed to comply with the instruction, its access to service would be blocked.[498] Two other courts suggested that the following conducts may fulfill the "control" requirement: 1) being "actively involved in the listing, bidding, sale and delivery" of items offered for sale;[499] 2) controlling vendor sales by previewing products prior to their posting, editing product descriptions, or suggesting prices.[500] A court even connected the "right and ability to control" with the specific knowledge of infringement, and held that "the right and ability to control

494 A decision made by the District Court of S.D. New York was an exception, and in this case the court held that "the ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise." See *Arista Records LLC v. Usenet.com, Inc.*, 633 F.Supp.2d 124, at 157 (S.D.N.Y.2009).

495 See *Viacom International, INC. v. YouTube, INC.* (n7), at 36-38. In this case, the court summarized all decisions about the control provision in the DMCA 512 (c)(1)(B), and concluded that the prior case law completely agreed with the opinion that the control provision required something more than the "ability to remove or block" the hosted content.

496 According to the "notice-and-takedown" mechanism, once a hosting ISP receives a competent notice about infringing content, it should expeditiously remove or disable access to material alleged to be infringing. Therefore, the DMCA 512 has already implied that a qualified hosting ISP should have the right and ability to remove or disable access to materials posted on its website. A similar analysis can also be found in the relevant US case law. For example, in the case of *Hendrickson v. Ebay Inc.*, the Court stated that: "Congress could not have intended for courts to hold that a service provider loses immunity under the safe harbor provision of the DMCA because it engages in acts that are specifically required by the DMCA." See *Hendrickson v. Ebay Inc.*, 165 F. Supp. 2d 1082, at 1093-1094. (C.D. Cal. 2001).

497 See *Viacom International, INC. v. YouTube, INC.* (n7), at 38.

498 See *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, at 1173 (C.D. Cal. 2002). In this case, the Cybernet ran a web-service called "Adult Check", and the plaintiff, Perfect 10, was a corporation owning copyright over considerable pornographic content. During the hearing, the court was unsure about whether Cybernet was a qualified ISP. However, the court held that even with the assumption of Cybernet's qualification as an ISP, Cybernet could still not enjoy the shield of the "safe harbor" provision, because it failed to conform to the DMCA 512(c)(1)(B).

499 See *L'Oréal SA and Others v eBay International AG and Others* (n327), at 1094.

500 See *Corbis Corporation v. Amazon.com, Inc.* (n333), at 1110.

the activity requires knowledge of it, which must be item-specific."[501] By examining the factors listed above, it can be concluded that the US courts set a very high standard for control provision in the DMCA §512(c)(1)(B), and consequently the normal hosting ISPs without actively being involved in choosing posted contents can hardly meet the threshold of "control". Furthermore, a hosting ISP which commits an inducing infringement is highly likely to fulfill both elements of "control" and "direct benefits".[502]

To sum up, although the provision in the DMCA §512(c)(1)(B) can be seen as originating in vicarious liability in common law, it should be interpreted as being less strict when applied to hosting ISPs, because it is set to limit the hosting ISPs' liability. Along with this track, the US courts mainly focus on defining which benefit is not directly attributable to infringement and which conduct is not a "control" rather than defining what constitutes direct benefits and "control". Therefore, hosting ISPs running a normal commercial model, such as Veoh, YouTube and Amazon, are still qualified for the DMCA §512(c)(1)(B).

4.4.2 Benefit in the EU

Unlike the DMCA 512, the E-Commerce Directive does not prescribe whether hosting ISPs benefit from infringement is a factor to be considered when deciding whether hosting ISPs can enjoy the liability exemption.[503] Nevertheless, the courts in member states do take into account whether hosting ISPs benefit from infringement when deciding on their liability for copyright infringement, which will be discussed in the following section.

120

4.4.2.1 Germany

Whether a hosting ISP receives benefit from copyright infringement is not an independent culpable element in Germany, because neither TMG § 10 nor general tort law rules clearly forbid receiving benefits, but German courts do take it into account when deciding whether a hosting ISP should be liable for direct user infringement.

In Germany the courts can deem a hosting ISP as a content provider and, thus, directly liable for infringement ("die Haftung als Content-Provider fuer eigene

501 *Viacom International, INC. v. YouTube, INC.* (n2), at 527. This conclusion has been overturned by the Appeal Court, since if setting the knowledge of specific items as a precondition of having right and ability to control, the DMCA 512(c)(1)(B) would be superfluous. "Any service provider that has item-specific knowledge of infringing activity and thereby obtains financial benefit would already be excluded from the safe harbor under § 512(c)(1)(A) for having specific knowledge of infringing material and failing to effect expeditious removal. No additional service provider would be excluded by § 512(c)(1)(B) that was not already excluded by § 512(c)(1)(A)." see *Viacom International, INC. v. YouTube, INC.* (n7), at 36.

502 The detailed discussion can be found in the following Section 4.5.1. "inducement liability in US".

503 Peguera, 'The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems' (n175), at 491.

Inhalte"). When deciding whether a hosting ISP should be treated as a content provider from a legal perspective, the German courts always refer to the factor of receiving a benefit. For instance, in a case about a platform for photograph exchange, the KG Berlin (Berlin Court of Appeal) concluded that the defendant ran the platform as a content provider, and one of the reasons was that: the defendant received 40 percent of the fees paid by the users who downloaded the photographs, and the rest of the fees were passed on to the users who offered those photographs for sale.[504] In another case about the video-sharing website YouTube, the LG Hamburg (Higher Regional Court of Hamburg) found that "YouTube commercially exploits the uploaded videos by selling ads space" was one of the reasons to hold YouTube as a content provider.[505] However, only receiving benefits from infringing content cannot lead a hosting ISP to be liable, because the German Federal Court of Justice set a quite strict pre-condition to make benefit be imputed in the case of *Marions v. Kochbuch*.[506] In this case, the German Federal Court of Justice emphasized that whether the defendant selected, checked, edited and integrated the up-loaded contents into its website should be deemed as the core factor to conclude the defendant's liability as a content provider, and the other facts, such as the requiring of rights transfer and receiving benefit, are only supportive evidence to conclude the liability.[507] By examining the decision of the German Federal Court of Justice, one finds that "die Haftung als Content-Provider fuer eigene Inhalte" is to some extent comparable to the DMCA §512(c)(1)(B) in the US, because integration of up-loaded content into its website can be seen as having the right and ability to control infringement, and the benefit received by a hosting ISP through integrating infringing content into its website can definitely be seen as directly attributable to infringement.

121

504 KG: Internetplattform zum Austausch von Fotodateien (n245), at 204. The other three reasons are as follows: 1) in particular, the uploaded photographs went through a selecting and checking procedure before they were publicly accessible; 2) the copyright owners of the photographs were pointed out but in an unnoticeable and indiscreet way; 3) in the front part of the website, the corresponding philosophy of the operator was displayed under its logo, which was "publish modern and time-spiritual photos".

505 LG Hamburg: Haftung eines Plattformbetreibers – YouTube (n247), at 834. The other reasons are as follows: 1) the logo of YouTube appeared on the upper right corner of videos because of a pre-designed website frame, when the downloadable videos were on play, but by contrast the signs or pseudonym of the uploading-users were very small and appeared on a separate part of the website apart from the videos; 2) the defendant sorts the uploaded videos into different categories, and when a video is clicked, the similar videos will show up on the right side of the webpage automatically; 3) YouTube requires the up-loaders to grant it the right to use these videos.

506 BGH: Verwendung fremder Fotografien für Rezeptsammlung im Internet – marions-kochbuch.de (n250), at 1276-1278. Case reference: BGH, Urteil vom 12. 11. 2009 - I ZR 166/07. In this case, the defendant operated a website called chefkoch.de for the public to upload cooking recipes and corresponding photographs and the plaintiff ran a website called marions-kochbuch.de which introduced cooking recipes with relevant pictures. The plaintiff found that some of his copyrighted cooking instructions had been uploaded to the defendant's website, so he launched a suit against the defendant for copyright infringement.

507 Ibid, at 1276.

4.4.2.2 *France*

As being referred above, according to Article 6 of LCEN, whether a hosting ISP should be held liable depends whether it has actual knowledge of the infringement at issue, and whether a hosting ISPs receives profits is irrelevant when deciding liability. However, maybe because French judges consider the facts from the victim's common sense[508] and were influenced by US law,[509] receiving profits had been held as a culpable element by French courts. In this respect, French courts adopted a similar approach to German courts which took receiving profits as a reason to categorize hosting ISPs as publishers or entities similar to publisher from the legal perspective. In the case of Tiscali, the defendant Tiscali was held as either a publisher or providing a service that went beyond mere technical functions, since Tiscali benefited from renting advertising space.[510] In another case, Myspace was held as a publisher for the same reason.[511] These decisions were criticized as inconsistent with French law, since the two French Acts (Freedom of Communication Act and LCEN) clearly state that the safe harbor defense covers the hosting service, either free of charge or for a fee.[512] Besides, since lots of hosting services are provided for free, hosting providers have to be financed by cross-subsidizing, such as selling ad space.[513] Eventually, the French court changed their judicial thought on this issue. In the case of Dailymotion, the French Supreme Court held that Dailymotion's use of a website for displaying ads
122 was just a way to make profit, and would not influence the uploaded content, so displaying ads would not transform Dailymotion into a publisher.[514]

4.4.2.3 *Italy*

In Italy, as what occurred in Germany and France, benefiting from copyright infringement had been held a reason to refuse hosting ISPs a "safe harbor". For instance, in the case of *Reti Television Italiane (RTI) v. IOL and Yahoo!*, the plaintiff RTI found that some of its television programs were unlawfully uploaded on the video-sharing

508 Copyright owners, as the victims, commonly believe that it is unfair for hosting ISPs to benefit from large number of visits attracted by the contents copyrighted by them.

509 Nérisson, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in France' (n103), at 79.

510 Matulionyte and Nérisson, 'The French Route to an ISP Safe Harbor, Compared to German and US Ways' (n231), at 58. Case reference: First Civil Division of the Supreme Court, 14 January 2010, Case No. 06-18855, 2010 Bull. civ. I, No. 8. In this case, profiting from selling ad space was just one reason to hold Tiscali as a publisher, and the other reason is allowing users to establish their personal pages. See discussion in the previous chapter.

511 Workman SW, Internet Law - Developments in ISP Liability in Europe, IBLS, *available at* http://www.ibls.com/internet_law_news_portal_view.aspx?id=2126&s=latestnews (last visited 01-03-2014).

512 Nérisson, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in France' (n103), at 79.

513 Ibid.

514 Blocman A, *Liability of Video-sharing Platforms - First Judgement of Court of Cassation*, IRIS Merlin(2011), *available at* http://merlin.obs.coe.int/iris/2011/3/article18.en.html (last visited 03-08-2014).

website run by IOL and Yahoo!, so the RTI sued IOL and Yahoo! for copyright infringement.[515] Since the defendants "provided for a system that allowed the publication of advertising links related to the videos," the District of Milan held it as one reason to conclude the defendant was acting as an active hosting provider, so the defendant could not enjoy the liability privilege set forth by the Article 14 and 15 of the E-commerce Directive.[516] In another case, YouTube was also held as an active hosting provider by the District of Rome, and one of the reasons was that YouTube organized the infringing content so as to make more revenue from ads.[517] In 2011, the Court of Milan even held that the E-commerce Directive was already out of date, since it did not take into account that the hosting providers who were "not merely passive and neutral with respect to the organization of the management of the contents published by the users but active in the management of such contents from whose advertising exploitation it gained profits."[518]

As an active hosting ISP, since a high number of videos were uploaded every day, it was not obligated to undertake ex ante monitoring on all uploads, but it still needed to undertake a higher level of duty care than a passive one.[519] For example, an unspecific notice "from a party alleging to be a right holder and merely mentioning the types of programs infringing its rights would have been sufficient to trigger an obligation to control and likely remove the infringing videos."[520] Recently, Italian courts seem to have loosed their standard on "active hosting". In the case of *Delta TV v. YouTube*, the District Court of Turin held that no sufficient evidence had been given to demonstrate YouTube as an active hosting ISP.[521] But obviously, YouTube are still making profits by selling advertising spaces. Therefore, in the view of District Court of Turin, making profits is not an important factor to hold a hosting ISP as "active" anymore.

To sum up, at the beginning, making profits, such as selling ad spaces, had been viewed as an imputed factor to hold hosting ISPs liable in France, Germany and Italy. Nevertheless, the courts in these three Member States have already lowered their criteria on imputed benefiting, and getting revenues through a normal business model, such as selling ad spaces, is not an imputed factor anymore. In fact, this change in these

515 Bellan, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in Italy' (n238), at 108.

516 Bonadio & Santo, 'Court of Milan holds video sharing platforms liable for copyright infringement' (n239), at 15.

517 Bellan, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in Italy' (n238), at 110.

518 Decision of the Court of Milan of January 20, 2011 No.27079/09, quoting Coraggio, 'Google's victory might be a short success' (n442), at 139-140.

519 Bellan, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in Italy' (n238), at 111-112.

520 Coraggio, 'Google's victory might be a short success' (n442), at 140.

521 Spedicato, 'Italy: the take-down notice must contain the specific YouTube URLs' (n437).

three jurisdictions conforms to *Adwords* Decision made by the ECJ, because in this decision, the ECJ clarified that merely setting the payment terms or providing general information to its clients cannot have the effect of depriving Google of the exemptions from liability provided for in Directive 2000/31.[522] The Advocate General in this case even argued that, "information society services will rarely consist of activities which are exclusively technical, and will normally be associated with other activities which provide their financial support."[523] Therefore, generally, benefiting has become a less important factor when deciding on hosting ISPs' liability in the EU.

4.4.3 Direct Benefit in China

Article 22 of the Regulation provides that a hosting ISP can be exempted from monetary remedy if it fulfills certain requirements, one of which is "not receiving benefit directly attributable to infringements". Since neither Chinese tort law rules nor Chinese Copyright Law had categorized benefits into direct and indirect, the concept of "direct benefit" in Article 22 has obviously been introduced from the DMCA 512(c)(1)(B). However, for some unknown reason, the other element of "right and ability to control" has not been integrated into Article 22. Faced with this new concept of "direct benefit", the Chinese courts seem to be unsure about how to interpret it, and some courts have even reached completely different conclusions
124 when interpreting similar facts.

In China, the public is generally free to use most hosting services, so a hosting ISP will mainly make a profit by selling advertising space on its website. This raises the question of whether this kind of benefit should be affirmed as directly attributable to infringements. In the case of "*BuSheng v. YoBo*", the Haidian District Court in Beijing concluded the existence of direct benefits based on the following analysis: the infringing music on the defendant's website attracted more people to visit its website, so the defendant could make more profit by selling advertising space.[524] In contrast, in another case, "*CiWen v. 56.com*", the Beijing Second Intermediate People's Court concluded that all of the videos on the defendant's website could be viewed for free, and although an advertisement was being displayed with a copyrighted work owned by the plaintiff, there was insufficient evidence to prove that the benefit received by the defendant in this case was directly attributable to this

522 *Google France SARL and Google Inc. v Louis Vuitton Malletier SA and Others* (n230), at para. 116.

523 Opinion of Advocate General, *Google France SARL and Google Inc. v Louis Vuitton Malletier SA and Others*, joined cases C-236/08-C-238/08, at para. 339.

524 *BuSheng v. YoBo (步升v.友播)*, Beijing Haidian District Court (北京市海淀区法院), No. 6939 Hai Min Chu Zi(2008) (（2008）海民初字第6939号). In this case, the plaintiff BuSheng owned copyright of certain musical works, some of which had been uploaded to the defendant's websites by Internet users, so the plaintiff sued YoBo for copyright infringement.

copyrighted work.[525] In limited cases, the court has concluded a hosting ISP's liability based on selling advertising space even without considering whether it constitutes direct benefit or not. For example, in the case of "*joy.cn v. 56.com*", the Haidian District Court held that, since the defendant "56.com" had profited by displaying advertisements with the uploaded content, it needed to undertake a higher level of duty of care to check for potential copyright problems among the uploaded content; however, the defendant had not fulfilled this kind of duty of care, so it should be liable.[526] Furthermore, Article 22 of the Regulation also requires hosting ISPs not to alter the works, performance, sound or video recordings that are provided by the service recipients. Some Chinese courts have held that displaying advertisements with uploaded contents forms a sort of alteration in the context of Article 22, and have thus expelled hosting ISPs out of "safe harbor". For example, in the case of "*joy.cn v. 6room.com*", the HaiDian District Court concluded that, since before and after the playing of alleged infringing videos, 6room.com displayed advertisements, and whenever a viewer clicked on the pause-button, an advertisement would also appear, so the defendant had actually altered the alleged infringing videos supplied by Internet users when it added advertisements.[527]

Today, however, the Chinese courts no longer seem to be treating "display advertisements" as an "alteration". According to a Guiding Opinions published by the Beijing Higher Court,[528] "displaying the advertisement before or after the playing of the works, performance, sound or video recordings, or popping up ads during the playing of the works, performance, sound or video recordings" should not be found as alteration of uploaded contents.[529] Moreover, the Internet Provisions promulgated by the People's Supreme Court include a detailed provision about what constitutes direct benefit, which states the following:

525 *CiWen v. 56.com (慈文v.56网)*, Beijing Second Intermediate People's Court (北京市第二中级人民法院), No. 9 Er Zhong Min Zhong Zi (2008) (（2008）二中民终字第9号). In this case, a television series call "Jia" (Family) owned by the plaintiff CiWen had been uploaded to the defendant's website "56.com" without permission, so the plaintiff sued "56.com" for copyright infringement.

526 *joy.cn v. 56.com (激动网v.56网)*, Beijing Haidian District Court (北京市海淀区法院), No. 24750 Hai Min Chu Zi (2008) (（2008）海民初字第6939号). In this case, some copyrighted videos owned by the plaintiff "Joy.cn" had been uploaded to the defendant's website "56.com" without permission, so the plaintiff sued "56.com" for copyright infringement.

527 *joy.cn v. 6room.com (激动网v. 六房间)* (n222).

528 This Guiding Opinions (n229) is not a mandatory legal document, because unlike the People's Supreme Court in China, the Beijing Higher People's Court has no statutory rights to promulgate any judicial interpretation of general application. However, Beijing, as one of the two cities (the other is Shanghai) hearing most of the disputes about Internet copyright infringement in China, the courts there always take a lead in solving these disputes and have accumulated considerable judicial experience in this respect. Therefore, the Guiding Opinions provided by the Beijing Higher People's Court definitely has widespread influence in China and will be used as an important reference by other courts.

529 Ibid, Art. 24 (3).

> where service providers make profits by displaying advertisements along with specific works, performances or sound or video recordings, or receive other financial benefits which are specifically related to the works, performances or sound or video recordings transmitted by them, it should be concluded that the service providers receive direct financial benefits; however, the normal advertising fee or service fee collected by service providers on the basis of offering an Internet service cannot be identified as direct benefit.[530]

Therefore, where selling advertising space is regarded as receiving direct benefits, a specific relationship should exist between advertisements and the content with which they are displayed. This kind of specific relationship indicates that service providers have a certain ability to control the uploaded content, since the service providers should specify the content before displaying any advertisement with it. Consequently, although the Internet Regulation does not restrict "receiving direct benefits" with the element of "control", the Chinese courts have already realized that "receiving direct benefits" should be interpreted strictly and that service providers should at least have some sort of control over the uploaded content when concluding that they directly benefit from selling advertising space.

To sum up, the US "safe harbor" provision requires a hosting ISP not to receive direct
126 benefit from infringement when it can control the infringing activities. It seems that the US courts interpret the "receiving direct benefit" prong by referring to vicarious liability in common law, but since the "control" prong has been quite strictly interpreted, in just a few cases the hosting ISPs were blocked outside of "safe harbor" because of making profits through their services. In Germany, France and Italy, "receiving benefit" is one factor used to hold a hosting ISP liable as a content provider. However, in the case of Adwords, the ECJ held Google not liable for making profits by selling Adwords service.[531] Then, in Germany, "receiving benefit" became merely supportive evidence to render hosting ISPs liable as content providers. In France and Italy, making a profit through a common business model also cannot result in hosting ISPs' liability anymore. In China, although the Chinese "safe harbor" provision does not prescribe a "hosting ISPs' ability to control infringements" as a restriction to the element of "receiving direct benefit", the "control" requirement has already been indicated in the Internet Provisions issued by the People's Supreme Court. Ultimately, in the US, EU and China, a hosting ISP cannot be held liable because it simply operates a normal advertising business without choosing with which content the advertisements are displayed.

530 See Internet Provisions (网络规定) (n208), Art. 11.

531 *Google France SARL and Google Inc. v Louis Vuitton Malletier SA and Others* (n230), at para. 116.

4.5 Inducement Liability

Since a service provider's liability cannot be concluded from its offering a service which is capable of substantial non-infringing use, the service provider's intent could be an important reference for courts in deciding its liability. This is because the "safe harbor" provision does not aim at fostering copyright infringements. Therefore, if a service provider encourages or induces its users to commit infringements with illegal intent, then it is probably barred from the "safe harbor" provision and, thus, liable for primary infringements. This section examines the role of inducement and illegal intent in deciding a hosting ISPs' copyright liability.

4.5.1 Inducement Liability in the US

In *Grokster*, the US Supreme Court adopted inducement liability into the field of Internet copyright against a p2p software called Grokster. Inducement liability can be concluded under either of these two circumstances: 1) "actively encouraging (or inducing) infringement through specific acts"; 2) "distributing a product distributees use to infringe copyrights, if the product is not capable of 'substantial' or 'commercially significant' non-infringing uses."[532] As for the former circumstance, it can be further described as distributing "a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps to foster infringement."[533] After *Grokster*, several cases about p2p software have been decided by taking advantage of inducement liability as established in *Grokster*,[534] but the relationship between inducement liability and "safe harbor" provision was substantially discussed until the "*Fung*" case.

In the case of *Columbia v. Fung*, the defendant Fung ran several websites including www.isohunt.com, www.torrentbox.com, www.podtropolis.com, and www.ed2k-it.com, which allowed users to download files to their computers.[535] The plaintiff claimed that with the facilitation of Fung's websites, users could easily download "infringing copies of popular movies, television shows, sound recordings, software programs, video games, and other copyrighted content free of charge," and some of these contents were copyrighted by the plaintiff, so the plaintiff sued Fung for copyright infringement.[536] In the first instance, the Court held the defendant Fung contributorily liable for its inducement of copyright infringement on the following grounds: 1) the defendant's message to users demonstrated its consistent intent to promote the infringing use of its service, such as setting special pages for users to

532 *MGM Studios Inc. v. Grokster Ltd.*, 545 U.S. 913, at 942 (2005).

533 Ibid, at 913.

534 *Arista Records LLC. v. Lime Group LLC*, 784 F. Supp. 2d 398, at 424 (S.D.N.Y. 2011). This is a case against p2p software, and since running p2p software is not a typical internet service covered by "safe harbor" provision, the court need not discuss the relationship between inducement liability and the "safe harbor" provision.

535 *Columbia Pictures Industries, Inc. v. Gary FUNG*, 2009 WL 6355911 (C.D. Cal.), at 1.

536 Ibid.

upload dot-torrent files about top popular movies; 2) the defendant assisted its users to engage in infringement; 3) the defendant implemented the technical measures to promote copyright infringement; 4) the defendant's business model depended on massive infringing use.[537] When facing the defendant's assertion of its qualification for the "safe harbor" provision, the court stated that "inducement liability and the Digital Millennium Copyright Act safe harbor are inherently contradictory." This is because inducement liability results from bad faith conduct with a purpose of promoting infringement, but the "safe harbor" provision aims at protecting the legal e-business run in good faith.[538] Therefore, the district court in the "Fung" case appeared categorically to bar inducement liability from the "safe harbor" provision.[539]

In "*Columbia v. Fung*", on appeal, the 9th Circuit Court also started by comparing this case with *Grokster*, and then concluded that the defendant, Fung, had fulfilled every element of inducing infringement, including the distribution of a device or product, acts of infringement by Internet users, with the object of promoting its use for infringing copyright and causation between infringements and inducing. Hence, Fung needed to undertake inducement liability.[540] However, when coming to the relationship between inducement liability and the "safe harbor" provisions, instead of holding that inducement liability could be categorically excluded from the "safe harbor" provision, the 9th Circuit mentioned the possibility that a hosting ISP who committed inducement could still be shielded from liability.[541] However, the 9th Circuit still found the defendant *Fung* liable, because he failed to meet "safe harbor" provision for host or information tools ISPs.[542] To be precise, Fung was "aware of facts or circumstances from which infringing activity was apparent," and received a benefit directly attributable to the infringing activity where he had the "right and ability to control such activity."[543]

The 9th Circuit held that the defendant had the "red flag" knowledge of infringement on the basis of his particular inducing activities: the record was "replete with instances of Fung actively encouraging infringement, by urging his users to both

537 Ibid, at 9-15. In this case, the defendant, Fung, ran several websites which would "collect, receive, index, and make available descriptions of content, including so-called 'dot-torrent files,' and would also provide access to 'open-access' BitTorrent Trackers." Consequently, the district court denied treating the defendant's service as a transitory digital Internet communication or host rather than an information location tool. However, the court made a clear statement about the relationship between inducement liability and the "safe harbor" provision, so it is still relevant to the discussion here. Moreover, in the appeal instance, the 9th Circuit held that the defendant could be seen as a hosting ISP.

538 Ibid, at 18.

539 See Reese RA, 'The Relationship Between the ISP Safe Harbors and Liability for Inducement' (2011) 8 Stanford Technology Law Review 1, at 3.

540 See *Columbia Pictures Industries, Inc. v. Gary FUNG*, 710 F.3d 1020, at 1032-1037. (9th Cir. 2013).

541 Ibid, at 1040.

542 Ibid.

543 Ibid, at 1047.

upload and download particular copyrighted works, providing assistance to those seeking to watch copyrighted films, and helping his users burn copyrighted material onto DVDs."[544] These materials were obviously copyrighted to a reasonable person and could not be "licensed to random members of the public" without any charge, because they were "sufficiently current and well-known".[545] Moreover, Fung also admitted that he had personally used the isoHunt website (one of the websites involved in this dispute) to download infringing materials.[546] Therefore, the 9th Circuit held that he had the broad "red flag" knowledge of copyright infringement.[547] As for the "receiving direct benefit from infringement" prong of § 512(c)(1)(B), the 9th Circuit based its opinion on the following facts: 1) Fung attracted advertisers by pointing advertisements to the infringing materials; 2) Fung induced and assisted these persons who committed infringement on his websites so as to attract more visitors to his websites; 3) Fung's revenue relied on the number of visitors to his websites.[548] Furthermore, the 9th Circuit also held that Fung had the right and ability to control the infringement, because 1) Fung organized and described the torrent files on his websites so as to make these high-likely infringing materials much easier to access; 2) Fung assisted users to locate the likely infringing materials that they could find themselves; 3) Fung personally removed disqualified torrents from his websites, such as fake or infected ones.[549] To sum up, even though the 9th Circuit refused to exclude inducement liability from the "safe harbor" provision categorically, a hosting ISP who commits an inducing infringement still seems to be highly likely to be barred from the "safe harbor".

4.5.2 Inducing Infringement in China

Hosting services are likely to be used for copyright infringement, so in order to prevent hosting ISPs from making more profit by promoting the infringing use of their services, Chinese Courts tend to hold hosting ISPs liable if they commit certain inducements. The Internet Provision issued by the People's Supreme Court reads that where service providers induce or encourage Internet users to infringe others' copyright by delivering words, offering technical support, or rewarding credits, the service providers shall be concluded to have committed inducing infringements.[550] In addition, the Guide for Hearing Copyright Disputes Involving Video-sharing

544 Ibid, at 1043.
545 Ibid.
546 Ibid.
547 Ibid. In this case, the 9th Circuit Court was still not entirely confident about "red flag" knowledge already being fulfilled, for the reason that it was uncertain whether exclusion from the § 512(c) safe harbor because of actual or "red flag" knowledge of a specific infringing activity applied only with regard to liability for that infringing activity, or more broadly.
548 Ibid, at 1045.
549 Ibid.
550 See Internet Provisions (网络规定) (n208), Art. 7.

(hereinafter "Guide") published by the Beijing People's Higher Court also provides that, where hosting ISPs, by taking advantage of their service models, induce or encourage internet users to infringe the rights of others' works, performances, sound or video recordings on the Internet, the hosting ISPs shall be held to have committed inducing infringements.[551]

Only a few months after the Internet Provision entered into force, a company which ran a BBS for Internet users to share content was held to have committed an inducing infringement in the case "*chineseall.com v. 178.com*". In this case, the BBS operated by the defendant "178.com" had a sub-platform for subscribers to upload ePub-formatted e-books, and a copyrighted book owned by the plaintiff had been uploaded without permission, so the plaintiff sued 178.com for copyright infringement. According to the court investigation, the defendant had a policy of rewarding these subscribers who uploaded content or replied to such content with virtual "silver coins", so ChaoYang District Court in Beijing held that the defendant had induced its subscribers to commit infringements.[552]

By examining the Internet Provision, Guide, and 178.com case, one can see that the Chinese Courts have a stricter rule against hosting ISPs which commit inducements than the US courts. First, unlike the 9th Circuit, which rejected setting inducement liability as a categorical exclusion from "safe harbor", the Chinese courts have already made it quite clear that an inducing infringement cannot enjoy the liability exemption provided in the "safe harbor" provision.[553] Second, even compared with the inducement liability criteria founded in "Grokster", the Chinese inducing infringement is easier to reach, because "Grokster" required the defendant to induce infringements by clear expression or other affirmative steps,[554] whereas in China a general or even indirect inducement can lead a hosting ISP to undertake liability, such as awarding virtual "silver coins" to those subscribers who upload content or make comments.[555]

130

4.5.3 Intent to Facilitate Infringement in the EU

In the EU, there is no specific category of copyright infringement called inducing infringement. However, it is commonly held by the tort law rules that if a person induces others to commit infringement, he/she must be liable for the infringement. For example, as provided in Article 830 of German Civil Code, the persons who

551 Beijing High People's Court (北京市高级人民法院), Guide for Hearing Copyright Disputes involving Video-sharing (视频分享著作权纠纷案件的审理指南), JingGaoFaFa[2012] No. 419 (京高法发[2012]419号), Art. 3.

552 *chineseall.com v. 178.com (北京中文在线v.北京智珠网络技术)*, Beijing Chaoyang District Court (北京市朝阳区人民法院), No. 8854 Chao Min Chu Zi (2013) (（2013）朝民初字第8854号).

553 In terms of the Provisions promulgated by People's Supreme Court, once the inducing infringement has been concluded, "safe harbor" provisions are not applicable anymore.

554 See *MGM Studios Inc. v. Grokster* (n527), at 913.

555 See *chineseall.com v. 178.com（北京中文在线v. 北京智珠网络技术)* (n547).

induce or contribute to the infringement should be seen as joint infringers.[556] In the UK, the person who "conspires with the primary party or procured or induced his commission of the tort" will be held liable as a joint tortfeasor.[557] Further, the UK case law has developed a concept named "Nelsonian knowledge" that is similar to the "willful blindness" in the US.[558] If a man deliberately "shut his eyes to the facts he prefer not to see", he should be held to have Nelsonian knowledge of these facts and therefore be liable.[559] Besides, the ECJ also indicates that hosting ISPs' intent can be taken into account when deciding their liability. In the case of *L'oreal v. eBay*, the ECJ stated that if eBay "provides assistance which entails, in particular, optimizing the presentation of the offers for sale in question or promoting them," it should be held liable.[560] But the ECJ did not make any further statement about what constitutes imputed intent. At national level, the courts in member states also take hosting ISPs' intent into account when deciding liability, and provide more detailed interpretation about imputed intent. The following section explores how national courts interpret imputed intent when dealing with hosting ISP's liability.

4.5.3.1 Germany

In Germany, in the final instance of *Rapidshare*, the Federal Court of Justice referred to hosting ISPs' intent and their commercial models when deciding how broad the hosting ISP's "Disturber's liability" should be.[561] It is worth noting that the same defendant, Rapidshare, faced different fates in two lawsuits which occurred in the US and Germany, respectively. In these two cases, *Rapidshare* had operated an online hosting service for users to upload and share their content. While Rapidshare itself did not offer a search tool or index contents for users who wanted to search for specific materials, its users could still easily find the infringing materials in Rapidshare through search tools run by others.[562] In the US, the S. D. Cal. Court held that Rapidshare's commercial model was tolerable, and it neither committed contributory infringement nor needed to undertake inducement liability.[563] However, the same commercial model seems problematic in the view of the German Federal Court of Justice. It first held that Rapidshare needed to assume "Disturber's liability" because its commercial model substantially induced large scale infringements.[564] Second, as for the scope of "Disturber's liability", Rapidshare should exert comprehensive and regular control over its "link collections", such as seeking out any infringing

556 Sterling, JAL, *World Copyright Law* (n97), at 629.
557 *Credit Lyonnais Bank Nederland NV v. Export Credits Guarantee Dept* [1998] 1 Lloyd's Rep 19, at 46.
558 *Twinsectra Limited v. Yardley and Others* [2002] UKHL 12, para. 112.
559 Ibid. In light of Lord Millet's understanding, Nelsonian knowledge amounts to actual knowledge.
560 *L'Oréal SA and Others v eBay International AG and Others* (n327), para. 123.
561 See what has been discussed in Section "Störerhaftung - disturber's liability in Germany".
562 *Perfect 10, Inc. v. RapidShare* (n6); see BGH – Rapidshare (n42), at 1.
563 Ibid, at 6-11.
564 BGH – Rapidshare (n42), para. (b).

"link collection" by taking advantage of general search machines such as Google, Facebook, and Twitter, and if necessary, proper web crawlers should also be used.[565]

4.5.3.2 *France*

In France, the Supreme Court held that if a defendant provided a product or service which manifestly intended to allow Internet users to communicate copyrighted materials without permission, the defendant should be liable.[566] In the case of *SCPP and SPPF*[567] *v. Mubility (Societe)*, the defendant ran the music streaming site "Radioblogclub.fr" which offered "an index system via hypertext links and a search engine" allowing its users to find the phonograms through the name of the artist or the work from a database available on the website radioblog.fr, and then to listen to them.[568] Further, as has been shown in the certified reports, the large majority of music available on the website "radioblog.fr" was definitely under copyright protection, since they were famous French or international light music works.[569] Besides, the defendant also promoted the software named "Radioblog" which could be downloaded from its website. With the help of "Radioblog", the users were allowed to search and index the music on website radioblog.fr, make up their own playlists, listen to them and transfer them onto the personal sites or blogs.[570] Based on the facts above, French Supreme Court held that the defendant provided
132 the internet service, especially the software, which "manifestly aimed at making protected works available to the public without authorization," and therefore, should undertake criminal liability.[571]

In this case, the defendant claimed that it could benefit from liability exemption as a hosting ISP, since the playlists of music on radioblog.fr were made up by Internet users, and it also implemented the policy that once a request was made for a phonogram to be taken down by the rights holder, the removal could be done immediately.[572] However, this claim was dismissed and French Supreme Court held that a host might not benefit from the liability exemption provided in the Article

565 Ibid, para. (c), para. 21.

566 Spitz B and Avocats YS, *France: Radioblog condemned to damages for over €1 million*, Wolter Kluwer(2012), *available at* http://kluwercopyrightblog.com/2012/11/13/france-radioblog-condemned-to-damages-for-over-e1-million/ (last visited 27-08-2014).

567 SPPF is the short name for Société des Producteurs de Phonogrammes de France, and SCPP is the short name for Société Civile des Producteurs Phonographiques. Both of them are copyright collective management organization in France, and in this case, a large amount of music managed by them was made accessible to the public without authorization through the defendant's service.

568 *M. Louvel , P. ; Mme Radenne , J. (Rapporteur), M. Arnould J., Mubility (Societe) v. Societe Des Producteurs De Phonogrammes En France (Sppf) (As Civil Parties)*, [2013] E.C.C. 22, 229. 235.

569 Ibid, at 232.

570 Ibid, at 236.

571 Ibid, at 232-236.

572 Ibid, at 235.

6.I.3 of LCEN, if it had actual knowledge of the unlawful materials but failed to expeditiously remove or block access to them.[573] Therefore, in the light of the French Supreme Court's ruling, if a hosting ISP intentionally provides a service or product which aims at facilitating copyright infringement, the hosting ISP is presumed to have actual knowledge of the copyright infringement and thus is liable.

4.5.3.3 UK

In the UK, the Court of Appeal held a hosting ISP who took active measures to help and induce Internet users to commit copyright infringement as an authorizer of the infringement or as a joint tortfeasor.[574] In the case of *Twentieth Century Fox Film Corp v. Newzbin Ltd*, the defendant Newzbin ran a website which enabled the registered members to search for a wide range of content hosted on Usenet, and with lots of measures done by Newzbin to facilitate the search, many TV programmes and movies copyrighted by the plaintiffs could be easily found and downloaded from the Usenet, so the plaintiff sued Newzbin for copyright infringement.[575] Before discussing the court's decision, it is necessary to look into how Newzbin operated. Usenet allows its users to upload and view messages on an electronic equivalent of public bulletin boards which was mainly designed to deal with text materials of relatively small size.[576] Therefore, for the binary materials, such as films, which are substantially larger than text materials in size, they need to be encoded in a text form and then split into multiple parts so that they can be posted on newsgroup.[577] But each of these multiple parts is posted on the newsgroup separately, so a film may be distributed across hundreds or thousands of parts, which makes it quite time-consuming for Internet users to download a whole movie from Usenet.[578] Newzbin retrieved the messages that were scattered on a range of Usenet newsgroups by the title information, and provided three forms of indices which helped users find out all relevant messages of a film.[579] Especially, in order to provide the Newzbin index, 250 "editors" were required to make the reports about films, and ensure that each report includes all of the individual messages that comprise a copy of a film or other binary work and relevant descriptive information.[580] Further, Newzbin developed a facility for its premium members to create NZB files, and each NZB file contained all the information a news client required to fetch all the Usenet messages and reassemble the original binary work from its component parts.[581]

573 Ibid, at 236.
574 *Twentieth Century Fox Film Corp v. Newzbin Ltd* (n453).
575 Ibid, para. 1 to para. 4.
576 Ibid, para. 6, para. 10.
577 Ibid, para. 10.
578 Ibid, para. 13.
579 Ibid, para. 23-27.
580 Ibid, para. 27.
581 Ibid, para. 29.

Therefore, Newzbin immensely facilitated users to search and download films and other binary works from Usenet. Besides, the evidence showed that it would be straightforward for the Newzbin to restrict access to the movie and TV categories of binary content, but rather than to do so, the Newzbin in fact focused on facilitating the access to binary content.[582]

Based on Newzbin's operation activities, the Court of Appeal held the Newzbin as an authorizer of copyright infringement. By referring to Section 101(1) of the Australia Copyright Act, the court held that when deciding on authorization infringement, the following factors should be considered: the nature of the relationship between the alleged authorizer and the primary infringer, whether the equipment or other material supplied constitutes the means used to infringe, whether it is inevitable to be used to infringe, the degree of control which the supplier retains and whether he has taken any steps to prevent infringement.[583] First, regarding the relationship between Newzbin and it members, premium members paid Newzbin weekly, and then were allowed to use the searching and indexing facility provided by Newzbin to find the binary works on Usenet.[584] Second, with regard to binary works, Newzbin identified all of the, perhaps several thousand, messages which made up a particular binary work and, in so doing, saved premium members the very substantial task of manually locating and identifying each of them separately, so Newzbin provided its premium members the facility that went considerably beyond indexing and categorization.[585] Third, Newzbin provided a facility for its premium members to create NZB files, and upon pressing a button, the NZB files would be delivered to and stored at members' personal computers. If these NZB files consisted of copyrighted works, the infringement would inevitably occur.[586] Forth, Newzbin organized its indexing database into different categories in terms of the subject matter, and a very large proportion of the content in movie category was commercial and so very likely to be protected by copyright. However, Newzbin did not take any filtering measures to prevent infringement, but rather encouraged its "editors" to make reports about movies.[587]

Further, the Court of Appeal also held Newzbin as a joint tortfeasor. To conclude whether a person is a joint tortfeasor, it needs to examine whether he/she participated with others in a common design to infringe.[588] Normally, mere (or even knowing) assistance or facilitation of the primary infringement is not enough, and the joint tortfeasor must have so involved himself in the tort as to make it his own.

582 Ibid, para. 79, 37, 49 and 50.
583 Ibid, para. 90.
584 Ibid, para. 98.
585 Ibid, para. 99.
586 Ibid, para. 100.
587 Ibid, para. 101.
588 Ibid, para. 103.

Therefore, a joint tortfeasor should have induced, incited or persuaded the primary infringer to engage in the infringing act or have a common design or concerted action or agreement with the primary infringer on a common action to secure the doing of the infringing act.[589] According to the decision delivered by the Court of Appeal, Newzbin operated a site which was designed and intended to make infringing copies of movies readily available to its premium members; the site was structured in such a way as to promote such infringement by guiding the premium members to infringing copies of their choice, and then provided them with the means to download those infringing copies by using the NZB facility; the activation of the NZB facility in relation to one of the claimant's copyright films would inevitably result in the production of an infringing copy; Newzbin had encouraged and induced its "editors" to make reports of films protected by copyright, including those of the claimants; Newzbin further assisted its premium members to engage in infringement by give advice through the sharing forums; Newzbin profited from the infringement; and finally, the claimants were not able to identify particular infringements made by particular members only because the defendants kept no records of NZB files they had downloaded.[590]

In the decision, the Court of Appeal did not mention the E-Commerce Directive, which provides ISPs with defense again civil and criminal liability for infringement committed by their users in certain circumstances.[591] Therefore, it seems that an ISP which actively induces and facilitates the Internet users to commit copyright infringement, not only should be held as the authorizer of infringement and joint tortfeasor, but also cannot benefit from the liability exemption.

To sum up, in the EU, the E-Commerce Directive does not include a provision dealing with hosting ISPs' intent and liability exemption. Nevertheless, at the judicial level, the ECJ indicates that an illegal intent to promote infringement can render hosting ISPs liable. In Member States, the courts also pay attention to hosting ISP's intent, when deciding hosting ISPs' secondary liability for copyright infringement. Generally, if a hosting ISP intentionally promotes the infringing use of its service or even actively induces Internet users to commit copyright infringement, it needs to assume secondary liability and cannot benefit from liability privilege.

Based on the discussion above, it can be found that although the courts in each jurisdiction have set different criteria about imputed inducement, there is a common tendency in the US, EU and China that the courts take hosting ISPs' intent and business models as important factors when deciding liability. In the US, inducing infringements

589 Ibid, para. 108.

590 Ibid, para. 111.

591 Shillito M and Meale D, 'Twentieth Century Fox Film Corp v Newzbin Ltd - copyright - online service provider held liable for copyright infringements of its users' (2010), 32 European Intellectual Property Review 67, at 68.

must be done by clear expression or other affirmative steps,[592] whereas in China a general or even indirect inducement can lead a hosting ISP to be liable, such as awarding virtual "silver coins" to those subscribers who upload content or make comments.[593] In the EU, an intention to induce or facilitate infringement will be highly likely to result in hosting ISPs' liability.

4.6 Chinese Approaches to Decide Hosting ISPs' Liability

In China, the People's Courts always decide hosting ISPs' liability by referring to whether they have fulfilled reasonable duty of care in preventing Internet users from uploading infringing content. As for what kind of duty of care is reasonable for a hosting ISP, that remains unclear in Chinese judicial practice. However, it is at least certain that in the following three circumstances hosting ISPs should undertake a higher level of duty of care: when creating a channel for users to upload movies and television series, when having famous works or hot-playing movies uploaded onto their websites, and when the works have been viewed over certain times.

4.6.1 Setting a Channel for Users to Upload Movies and Television Series

In order to make the uploaded content look well-organized, the operators of
136 video-sharing websites always divide their uploading channels into different categories which are usually labeled with "original",[594] "movies and TV series", "entertainment", "education" "music" and others.[595] According to the Chinese Courts, the operators of video-sharing websites have the right to design the layout of their websites, but creating a channel specifically for movies and TV series is problematic. For example, In the case of "*nubb.com v. Tudou.com*", the Shanghai Higher People's Court concluded that since the defendant, Tudou.com, had set an uploading channel for "movies and TV series" parallel with a channel entitled "original", it must have known that the channel "movies and TV series" would produce a high possibility of infringement. Therefore, it should have undertaken more duty of care over the contents in the channel "movies and TV series" and was thus liable.[596] This raises questions as to how far this kind of higher duty of care can reach. Some courts have even interpreted it as monitoring liability. For instance, in the case of "*GuanShi Culture v. 6room.com*", the HaiDian District Court in Beijing concluded that the defendant, 6room, had created a channel especially for movies

592 See *MGM Studios Inc. v. Grokster* (n527), at 913.

593 See See *chineseall.com v. 178.com (北京中文在线v.北京智珠网络技术)* (n547).

594 The "original" here means the videos made by amateur Internet users rather than professional producers.

595 This kind of division can be found on nearly all main video-sharing websites in China, such as "youku.com", "tudou.com", and "video.sina".

596 *nubb.com v. Tudou.com (新传在线v.土豆网)*, Shanghai High People's Court (上海市高级人民法院), No. 62 Hu Gao Min San (Zhi) Zhong Zi (2008) (（2008）沪高民三（知）终字第62号).

and TV series, which meant it obviously knew many professionally produced movies and TV series were being uploaded onto its website. Consequently, the defendant should have monitored the content being uploaded to the "movies and TV series" channel and thus was liable.[597] Interestingly, it is also a common practice for video-sharing websites, such as YouTube and Veoh, to create different channels (including a channel for films) for Internet users to categorize their uploaded content, but the US courts did not take this as a reason to require YouTube or Veoh to undertake a higher level of duty of care. Perhaps affected by the relevant US case law, the Internet Provision does not specify that setting a channel for "movies and TV series" will result in a higher level of duty of care.[598] However, the Provision leaves considerable room for the lower courts to interpret in their own way.[599] According to the Guide issued by the Beijing Higher People's Court, with regard to the works involved, performance or audio-videos found in the channel of "movies and TV series", it is assumed that the defendants (video-sharing website operators) should know that these contents are infringing,[600] which means the operators of video-sharing websites still need to undertake a kind of duty of care similar to monitoring the channels of "movies and TV series".

4.6.2 Famous Works and Hot-playing Audio-video Works

For hot-playing audio-video works, the Chinese courts have not given a clear definition, but by deducing from case decisions, hot-playing audio-video works generally mean those movies and television series which are popular and still playing at movie theaters or on regular television. Since in China the box office is still the main revenue source for most movie producers and given that audiences who can watch the movies on the internet might not pay to enter theaters, the Chinese courts require video-sharing websites to fulfill more duty of care so as to prevent hot-play movies from being uploaded. In the case of "*vale.com v. Tudou.com*", the Shanghai First Intermediate People's Court held that because the production of movies was costly, it was almost impossible for copyright owners to make them available on the Internet for free; therefore, video-sharing websites should bear a higher level of duty of care on movies, especially for those hot-play ones.[601] 137

597 *GuanShi Culture v. 6room.com (观视文化v.六房间)*, Beijing Haidian District Court (北京市海淀区法院), No. 31332 Hai Min Chu Zi (2008) (（2008）海民初字第31332号). The HaiDian District Court also drew a similar conclusion in another case "*GuanDianWeiYe v. Youku.com*", see No. 14023 Hai Min Chu Zi(2008).

598 See Internet Provisions (网络规定) (n208).

599 Art. 9 and 12 of the Provision list some instances where service providers should be presumed to "should know the infringements", and these two articles end with "other factors" to be considered, which leaves lower courts enough room to make their own judgments.

600 See Guide (指南) (n546), Art. 7(1).

601 *vale.com v. Tudou.com (网络互联v.土豆网)* (n320). In another case - *nubb.com v. Tudou.com*, the Shanghai Higher People's Court made a similar statement on protecting "hot-play movies", see *nubb.com v. Tudou.com (新传在线v.土豆网)* (n591).

As for what constitutes famous work, there is also no clear definition, which means courts must decide on a case-by-case basis. Once a work has been identified as being a famous work, a higher level of duty of care will be imposed on hosting ISPs. For instance, in the case of "*Hanhan v. Baidu*", the HaiDian District Court in Beijing first admitted that the defendant, Baidu, did not need to monitor the "Baidu Wen Ku" (a platform for Internet users to upload and share literature) operated by it. Moreover, when deciding whether the defendant should have known that an illegal copy of "Xiang" (a work copyrighted by the plaintiff) was being uploaded to "Baidu Wen Ku", the following factors were comprehensively considered: objectively accessing the current situation of "Baidu Wen Ku", the fame of Hanhan and his work "Xiang", and Baidu's actual capacity to anticipate and control infringing activities. Finally, the Court concluded that the defendant should have undertaken a higher level of duty of care on illegal copies of Hanhan's works, such as "Xiang", because of Hanhan's reputation and the wide influence of his works.[602] By contrast, in the case of "*JiaHua Culture v. 56.com*", even though the defendant "56.com" had created an upload channel called "movies and TV series", on the grounds that the movies concerned were neither hot-play ones or famous in China, the ChaoYang District Court in Beijing held that the defendant was not liable.[603]

The Internet Provision issued by the People's Supreme Court sets "the fame of works" as one of the factors to consider when concluding whether service providers should know about an infringement. Additionally, the Internet Provision also includes rules about "hot-play audio-video works", which state that hosting ISPs will be presumed to know of the existence of infringements in the following circumstances: where hot-play audio-video works are located on the homepages, other main pages, or other pages which can be easily accessed by hosting ISPs, or where hosting ISPs take the initiative to choose, edit, sort or recommend hot-play audio-video works, or set a special top list for them.[604] When examining these rules, they do not require hosting ISPs to undertake a higher level of duty of care than complying with the normal "red flag" test and not actively being involved in infringement. The Guiding Opinions published by the Beijing Higher People's Court also include a similar provision, but cover not only hot-play audio-video works, but also popular music, other types of well-known works, and the performances, sound or video recordings related to these famous works.[605] Further, in terms of the Guide issued

138

602 See *Han Han v. Baidu (韩寒v.百度)* (n42).

603 *JiaHua Culture v. 56.com (佳华文化v.56网)*, Beijing Chaoyang District Court (北京朝阳地区法院), No.20595 Chao Min Chu Zi (2013) (（2013）朝民初字第20595号).

604 See Internet Provisions (网络规定) (n208), Art. 12.

605 See Guiding Opinions (指导意见) (n229), Art. 19(1). According to Article 19(1), where the alleged infringing content includes hot-play audio-video works, popular music works or other types of well-known works, or the performances and audio-video products, and this content is located on the homepages, other main pages or other pages which can be obviously accessed by service providers, then the hosting ISPs should be presumed to know about this infringing content.

by the Beijing Higher People's Court, once hot-play audio-video works, performances, or sound or video recordings can be found on their websites, hosting ISPs can be presumed to know of the hot-play content (so should be liable).[606] Therefore, by deducing from the Guide, hosting ISPs should monitor the hot-play content so as to avoid being held liable. To sum up, it is commonly held that hosting ISPs should thus exert a higher level of duty of care on preventing the hot-play or famous content from being uploaded. However, when it comes to how high this specific duty of care should be, the People's Supreme Court does not require hosting ISPs to do more than simply comply with the "red flag" test, whereas the Beijing Higher People's Court asks hosting ISPs to at least monitor hot-play audio-video works, performances, sound or video recordings.[607]

4.6.3 Higher Duty of Care on the Works Being Viewed over a Certain Number of Times

In the case of *ZhongQinWen v. Baidu*, the plaintiff ZhongQinWen found some of its copyrighted works were available on the platform BaiduWenku run by the defendant, so the plaintiff sued Baidu for copyright infringement.[608] But Baidu claimed that the BaiduWenku was just a platform for Internet users to upload and share materials, and it had fulfilled a reasonable duty of care to prevent infringement on its platform, so it should not be held liable.[609] In the first instance, Beijing First Intermediate People's Court held that Baidu was incapable of monitoring all of the uploads and did not directly benefit from infringement, but should know the infringing uploads in question.[610] According to the decision, the defendant Baidu kept the viewing and downloading data of each uploaded text, and by using current technologies, it was reasonable for Baidu to execute a monitoring mechanism in the light of which, once an uploaded text has been viewed or downloaded more than a certain number of times, Baidu needs to inspect the potential copyright problems of the text, including contacting the uploader, checking whether the text is originally created by the uploader or legally authorized by the copyright owners.[611] In this case, the plaintiff's works had been viewed by a high volume of users, but Baidu failed to exercise its duty to examine the legal status of the plaintiff's works, so Baidu should know the plaintiff's works were illegally uploaded.[612] In the appeal instance,

606 See Guide (指南) (n546), Art. 8(1).

607 The courts in Beijing have jurisdiction over most copyright disputes on the Internet, so the Guiding Opinion issued by Beijing Higher People's Court strongly affects cases about hosting ISPs' liability.

608 *ZhongQinWen v. Baidu (中青文v.百度)*, Beijing First Intermediate People's Court (北京市第一中级人民法院), (2013)YiZhongMinChuZi, No. 11912 (（2013）一中民初字第11912号).

609 Ibid.

610 Ibid.

611 Ibid.

612 Ibid.

Beijing Higher People's Court upheld the decision in the first instance.[613] This case law in fact sets another duty for hosting ISPs to protect popular works. Because once a copy of a popular work is uploaded on a platform, it tends to attract more views and downloads. Therefore, it is quite useful in respect of protecting these popular works, if setting an obligation for hosting ISPs to examine the copyright status of uploads which have been viewed or downloaded more than certain times. Meanwhile, this case law also tries to avoid rendering too much duty of care on hosting ISPs, since hosting ISPs are merely obligated to examine a certain amount of popular uploads but not all of them. However, both Beijing First Immediate People's Court and Beijing Higher People's Court did not set a clear indication on deciding how many times of views or downloads is enough to trigger the examining duty, which makes hosting ISPs' liability uncertain.

4.7 Analysis on the Imputed Factors Evaluated in Case Law:

The previous sections compare how the courts in the US, EU and China interpret relevant factors, including no general monitoring obligation, knowledge of infringement, receiving benefits from infringements, taking necessary measures against repeat infringements and inducement of infringement, when deciding hosting ISPs' liability. Based on the comparison, some tendencies can be found regarding regulating the copyright liability of hosting ISPs in the US, EU and China. First, because hosting ISPs are not subject to a general obligation to monitor their services or actively seek infringing materials, it is not easy to prove their knowledge of infringement in the US and EU except when they receive competent complaints.[614] In China, based on the "should know" criterion developed by case law, hosting ISPs' knowledge of infringement is easier to prove, because this criterion not only covers the US "red flag" test, but also aims at regulating the hosting ISPs' business-model by requiring them to fulfill a certain level of duty of care. Second, "receiving benefits" as an imputed factor seems to have become less important than before. For example, in the US, with the restriction of having the right and ability to control infringing activities, hosting ISPs can barely be held liable even if they receive direct benefit from the infringements; in the EU, "receiving benefits" has already become a side-factor to be considered; in China, "receiving direct benefits" as an imputed factor can only be concluded in quite limited circumstances.

Third, hosting ISPs' intent has become a more prevalent factor when the respective courts conclude liability. For instance, in the US, "willful blindness" and inducing infringement have been frequently discussed when the courts hear the cases about hosting

140

613 *ZhongQinWen v. Baidu (中青文v.百度)*, Beijing High People's Court (北京市高级人民法院), 2014 GaoMinZhongZi, No. 2045, (（2014）高民终字第2045号).

614 In some jurisdictions including the US, France and the UK, a hosting ISP is held to know infringement, if it induces or intentionally facilitates the infringement. See Section 4.5.1 and 4.5.3.

ISPs' liability; in the EU, if a hosting ISP intentionally promotes the infringing use of its service or even actively induces Internet users to commit copyright infringement in a substantial scale, it may need to be liable; in China, a general inducement or even an indirect inducement can lead a hosting ISPs to be held liable. Further, the courts also tend to evaluate hosting ISPs' business models rather than simply checking whether their services are capable of non-infringing use or not. In Germany, if a hosting ISP's business model is more likely to result in infringements, it needs to take more effective measures to prevent these infringements. Fourth, although a general monitoring responsibility is strictly forbidden for hosting ISPs, a specific monitoring responsibility has been established in the EU, which basically works thus: once infringing content has been identified, the hosting ISP needs to monitor this specific content so as to prevent it from being uploaded again. In China, a similar kind of specific monitoring responsibility can also be found in the Internet Provisions and relevant case decisions. In addition, compared with the US and EU, China requires hosting ISPs to undertake a higher level of duty of care to prevent hot-play audio-video works, famous and popular works from being uploaded, which aims at offering better protection for such highly valuable content.

Based on the above observation, these factors, including intent, business model, specific monitoring obligation and better protection for highly valuable content, have become the main reasons to hold hosting ISPs liable in the US, EU and China. In the following section, analysis will be done on these imputed factors drawn from the case law regarding hosting ISPs' secondary liability, and examines how these factors ought to be interpreted so as to preserve maximum freedom for hosting ISPs to operate in the US, EU and China.

4.7.1 Intent and Business Model

Base on the case law discussed above, courts have started to examine hosting ISPs' intent, namely whether they intend to induce Internet users to commit infringement through their services, when deciding hosting ISPs' secondary liability. If one looks deeper into case law, the intent to induce can be divided into two categories which are specific intent to induce (US)[615] and general intent to induce (Germany, China)[616]. Regarding the specific intent to induce, it requires "actively encouraging (inducing) infringement through specific acts," such as "shown by clear expression or other affirmative steps taken to foster infringement."[617] In contrast, general intent to induce only requires indirect or even passive inducement, which can be deduced from hosting ISPs' business model.[618]

615 See Section 4.5.1 "inducement liability in the US".

616 See Section 4.5.2 "inducing infringement in China" and the Germany part in Section 4.5.3 "intent to facilitate infringement in the EU."

617 *MGM Studios Inc. v. Grokster* (n527), at 942.

618 As being discussed in Section 4.5.2, a Chinese court held BBS operator as inducer because it had a policy of rewarding these subscribers who uploaded content or replied to such content with virtual "silver coins." Further, as has been discussed in Section 4.5.3, in Germany, the Federal Court of Justice held that Rapidshare needed to undertake "Disturber's liability" because its commercial model substantially induced large scale infringements.

Generally, since hosting ISPs' services can be used for both lawful and unlawful purposes, it is reasonable to check whether hosting ISPs intend to induce infringement when deciding their secondary liability. Nevertheless, what level of intent to induce can lead to hosting ISPs' liability should be properly defined, or otherwise, the inquiry into hosting ISPs' intent may render unreasonable burden on them, which would negatively affect the development of new distribution and copying technologies.[619] In other words, hosting ISPs' freedom to conduct business may be inappropriately impeded.

From the perspective of ensuring hosting ISPs' freedom to invent and adopt new Internet technologies, specific intent to induce is a more suitable standard. First, this standard does not challenge the technologies that are capable of unlawful use, but focuses on examining ISPs' acts, namely, whether they actively encourage copyright infringement by using their services.[620] Further, this standard does not question the ISPs' business model, which allows ISPs to adopt the latest technologies to optimize their services.[621] For instance, in the "Fung" case, the court held that the nature of Fung's business model alone could not justify inferring bad intent to conclude inducement infringement.[622] By contrast, if a hosting ISP needs to be liable for their general intent to induce infringement, it may negatively affect the hosting ISP's freedom to employ new Internet technologies. This is because, for a hosting ISP running a service capable of both infringing and non-infringing use, any promotion of its service can be, in a broad sense, understood as inducing infringement. For instance, in China, a BBS operator was held as an inducer merely by awarding virtual "silver coins" to those subscribers who upload content or make comments.[623] By awarding virtual "silver coins," the defendant does intend to encourage subscribers to upload content which is highly likely to include infringing materials, so in this sense, the defendant induces copyright infringement.[624] However, such a broad interpretation of inducement will deter hosting ISPs from adopting new technologies or optimizing measures that can attract more users. In Germany, the court decided the scope of a disturber's liability by examining hosting ISPs' business models, and if the measures adopted by a hosting ISP increase the risk of the infringing use of its service, it needs to accept wider disturber's liability.[625]

142

619 Högberg SK, 'The Search for Intent-Based Doctrines of Secondary Liability in Copyright Law' (2006) 106 Columbia Law Review 909, at 913.

620 According to the Grokster decision, "suspect" product design alone does not give rise to inducement liability under Grokster. See *MGM Studios Inc. v. Grokster* (n527), at 938.

621 Reese RA, 'The Relationship Between the ISP Safe Harbors and Liability for Inducement' (n549), at 6.

622 *Columbia Pictures Industries, Inc. v. Gary FUNG* (n550), at 1032-1037. In this case, the court held Fung's business model as supportive evidence to conclude inducement infringement. Further, some technical features of Fung's service can promote copyright infringement, such as implement "spider" program that allows users to locate and obtain copies of dot.torrent files, but the 9th Circuit did not take it as a reason to hold Fund as an inducer.

623 See See *chineseall.com v. 178.com (北京中文在线v.北京智珠网络技术)* (n547).

624 Ibid.

625 *Germany: "Rapidshare III" - Telemedia Act secs.7(2), 10* (2014), 45 International Review of Intellectual Property and Competition Law 716, at 716.

This decision may persuade hosting ISPs not to adopt new technologies to optimize their services, such as search tools or contents index, since these measures will help to find infringing materials, which increases the risk of the infringing use of their services.

"Specific intent to induce" standard reflects the wisdom of "substantial non-infringing use" doctrine[626] which provides significant protection for innovation in technologies that are related to the use of copyrighted material[627]. In the light of "substantial non-infringing use" doctrine, if a technology developer invents a dual-use product or service that is capable of both infringing and non-infringing use, the technology developer will not be held liable for the infringement committed by users through the new technology.[628] Further, under the "substantial non-infringing use" doctrine, the quantity or proportion of non-infringing use is irrelevant, because the product or service in question merely needs to be capable of non-infringing use.[629] By contrast, as demonstrated above, a general intent to induce can be easily inferred by the fact that the product or service is widely used for infringing purpose. Although "substantial non-infringing use" seems to favor technology developers, it aims to "reconcile the need to give copyright owners effective protection for their works and the rights of others freely to engage in substantially unrelated areas of commerce."[630] If liability rules lead technology developers to be easily liable for the technologies they invent for exploring copyrighted materials, copyright owners would control the development of new technologies involving copyright exploration.[631]

To sum up, although it is rational to examine hosting ISPs' intent when deciding liability, the imputed intent should be narrowly interpreted for the sake of allowing hosting ISPs to adopt new technologies. Thus, the general intent to induce infringement cannot result in hosting ISPs' secondary liability. This suggestion seems unfavorable to copyright protection, but as noted by Ginsburg, copyright owners "should maintain sufficient control over new markets to keep the copyright incentive meaningful, but not so much as to stifle the spread of the new technologies of dissemination."[632] Further, allowing the application of new technologies can also benefit copyright owners, because "economic evidence strongly suggests that those unanticipated future benefits, or 'spillover' effects, often exceed the immediate value of most new technologies."[633] For instance, the Video Cassette Recorder (VCR), as a technology that copyright owners

626 *Sony Corp. v. Universal City Studios, Inc.* (n51), at 442.
627 Lemley and Reese, 'Reducing digital copyright infringement without restricting innovation' (n3), at 1356.
628 Ibid, at 1356.
629 *MGM Studio, Inc v. Grokster Ltd*, 380 F.3d 1154, at 1162 (9th Cir. 2004).
630 *Sony Corp. v. Universal City Studios, Inc.* (n51), at 442.
631 Lemley and Reese, 'Reducing digital copyright infringement without restricting innovation' (n3), at 1356.
632 Ginsburg, 'Copyright and control over new technologies of dissemination' (n34), at 1613-1614.
633 Lemley and Reese, 'Reducing digital copyright infringement without restricting innovation' (n3), at 1387.

tried to outlaw,[634] later created a new market for copyright owners to make tremendous profits.[635] Currently, hosting ISPs and copyright owners have reached many cooperation agreements, in light of which copyright owners can share the revenues of hosting ISPs.[636] Therefore, a narrow interpretation of imputed intent is not only capable of maximizing hosting ISPs' freedom to operate, but also may benefit copyright owners in a long run.

4.7.2 Repeat Infringement and Specific Monitoring

Although an infringing material can be removed through notice-and-takedown procedure, this procedure cannot prevent the infringing material in question from being uploaded again. Therefore, in order to avoid the endless notice-and-takedown circle, hosting ISPs have been required to take necessary measures against repeat infringement.[637] For the purpose of preventing repeat infringement, certain monitoring needs to be done on the contents uploaded by users so as to locate the possible repeat infringement. Nevertheless, the "safe harbor" provisions prohibit requiring hosting ISPs to undertake general monitoring obligations.[638] In order to reconcile this potential conflict, the US court held that, to identify and terminate repeat infringers, the ISPs did not need to track users in a particular way to or affirmatively police users for evidence of repeat infringement.[639] However, in the EU, the courts justify such monitoring on repeat infringement by naming it as "specific monitoring" so as to avoid the suspicion of violating the "non-general monitoring obligation" clause.[640] In Germany, once notified of infringing materials, a specific monitoring obligation will be imposed on hosting ISPs to take necessary and reasonable measures to prevent the identical infringement from occurring again.[641] Therefore, in the case of Rapidshare discussed above, the Germany Supreme Court held that it was proportionate to monitor "a single digit number of external websites" regarding one specific work.[642] Similarly, "notice and stay-down" mechanism in France required the hosting ISPs to take all necessary measures

144

634 *Sony Corp. v. Universal City Studios, Inc.* (n51). In this case, copyright industry tried to persuade the US Supreme Court to ban the sale of VCRs produced by Sony, but finally the US Supreme Court created the "substantial non-infringing use" doctrine, which confirmed the legality of selling VCRs.

635 Lemley and Reese, 'Reducing digital copyright infringement without restricting innovation' (n3), at 1387.

636 According to a series of self-regulation documents signed between hosting ISP and copyright owners, hosting ISPs share their profits with copyright owners. See section 8.2 in Chapter 8.

637 See repeat infringer policy, disturber's liability and notice-and-staydown discussed above in Section 4.3.

638 See DMCA (n1), Sec. 512 (m) (1), E-commerce Directive (n1), Art. 15.

639 *Io Group, Inc. v. Veoh Internets, Inc.* (n5), at 1143-1145.

640 Matulionyte and Nérisson, 'The French Route to an ISP Safe Harbor, Compared to German and US Ways' (n231), at 66.

641 'Germany: Teleservices Act, secs.8(2),11; EU E-commerce Directive, Arts.14(1) and (2); Trade Mark Act, sec.14(2),(3) and (4) - "internet auction" (Internet-Versteigerung)' (2005) 36 International Review of Intellectual Property and Competition Law 573, at 573.

642 BGH – *Rapidshare* (n42), Para. 53.

to monitor the materials which had been notified as illegal.[643] In China, when deciding whether a hosting ISP should know the infringement concerned, courts need to evaluate whether the hosting ISP take reasonable measures against repeat infringements made by the same internet user.

The specific monitoring obligation is also acknowledged by the E-commerce Directive and ECJ. In the light of Recital 47, a "non-general monitoring obligation" clause does not concern monitoring obligations in a specific case.[644] Further, according to the ECJ, any business, even legitimate ones, may be required to conduct specific monitoring as long as it does not put the business itself at risk.[645] However, the borderline between specific monitoring and general monitoring can be blurred in the light of case law in Germany and France, since any notice from copyright owners can trigger the specific monitoring obligations in these two jurisdictions. Further, the notices as such in fact can accumulate at a very fast rate, so eventually, in order to monitor these infringements specified by notices, it is highly likely that hosting ISPs need to conduct a wide-spread monitoring obligation on materials uploaded by users.[646] For this reason, the French Supreme Court dismissed the "notice-and-staydown" mechanism in 2012.[647] In addition, imposing a specific monitoring obligation on hosting ISPs can result in a well-known phenomenon "slippery slope" in the context of Internet intermediary liability, because once hosting ISPs are subject to the first monitoring obligation, then their monitoring obligations would grow like a snowball.[648] As noted by Schellekens, if a hosting ISP is already obligated to monitor a specific infringing material, it would be difficult for a court to uphold that the monitoring of another specific infringing material is not possible.[649] Therefore, the boundary between specific monitoring and general monitoring is not clear-cut, and a specific monitoring obligation is highly likely to force hosting ISPs to conduct the general monitoring in the end. Besides the overlapping concern of specific monitoring and general monitoring, specific monitoring may also cause cost concern. In order to fulfill the so-called specific monitoring obligation, a hosting ISP may need to adopt a sophisticated and costly monitoring system, which would stifle its freedom to operate. As noted by the ECJ in the case of *SABAM v. Netlog*, the plaintiff required Netlog to adopt a filtering system at its expense for the information stored on its servers so as to

643 Angelopoulos, 'Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe' (n91), at 264.

644 E-commerce Directive (n1), Recital 47.

645 *L'Oréal SA and Others v eBay International AG and Others* (n327), para. 144.

646 Angelopoulos, 'Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe' (n91), at 265.

647 Jasserand C, 'Hosting providers' liability: Cour de Cassation Puts an End to the Notice and Stay Down Rule' (2013) Journal of Intellectual Property Law & Practice 192, at 192-193.

648 Schellekens M 'Liability of internet intermediaries: A slippery slope?' (2011) SCRIPTed 8(2) 154, at 154-155.

649 Ibid, at 163.

block the exchange of files copyrighted by the plaintiff, but the filtering system as such was unnecessarily complicated or costly, and thus failed to strike a fair balance between the protection of copyright enjoyed by right holders and the freedom of conducting business by hosting ISPs.[650]

When dealing with a specific monitoring obligation, it is useful to explore why "safe harbor" provisions set restriction on ISP's monitoring obligations. First, ISPs need to process a vast amount of information every day, so in order to ensure the efficiency of the Internet, it is impossible for them to monitor all of the information transmitted.[651] Second, if forcing ISPs to implement very burdensome monitoring obligations, it would inappropriately impede ISPs' freedom of conducting legitimate business,[652] and eventually stifle the e-commerce that is promoted by "safe harbor" provisions. Therefore, when dealing with specific monitoring obligation, courts should take into account the following two factors: whether hosting ISPs are capable of conducting the required monitoring and whether imposing such monitoring obligations will inappropriately impede their freedom to operate. In this sense, how far a specific monitoring obligation can extend mainly depends on the hosting ISP's monitoring ability in each case. For example, YouTube has adopted a sophisticated monitoring system - Content ID which can sufficiently prevent the infringing uploadings.[653] But for the start-up hosting ISPs, adopting a monitoring system as such would be too costly for them, so if requiring start-up ISPs to adopt complicated monitoring systems, it "would effectively raise the barrier to market entry, stifling innovation."[654] Nevertheless, it may raise legal uncertainty, if defining hosting ISPs' specific monitoring obligations based on their monitoring ability. First, judges are not experts in Internet technologies, so they may be incapable of accurately assessing the monitoring ability of hosting ISPs. More importantly, Internet technologies are updated on an extremely fast track, so a specific monitoring obligation defined in one case may soon become outdated.

In addition, considering so much information needs to be processed by hosting ISPs every day, even specific monitoring has to be done by technical filtering. However, the accuracy of technical filtering has been widely criticized, particularly for its inability to accommodate fair use. Michael S. Sawyer asserts that given that fair use is even such a major challenge for the courts to evaluate, it is almost impossible for any technological solution to reach accurate determinations.[655] Electronic Frontier

650 *SABAM v. Netlog* (n311), para. 44-46.

651 Lemley, 'Rationalizing Internet Safe Harbors' (n21), at 101.

652 *L'Oréal SA and Others v. eBay International AG and Others* (n327), para. 140.

653 How Content ID works (n42).

654 Holland CBA, Hermes J, Sellars A, Budish R, Lambert M, and Decoster N, *NoC Online Intermediaries Case Studies Series: Intermediary Liability in the United States at* http://cyber.law.harvard.edu/is2015/sites/is2015/images/NOC_United_States_case_study.pdf (last visited 28-09-2014).

655 Sawyer MS, 'Filters, Fair Use & Feedback: User-Generated Content Principles and the DMCA' (n43), at 366. In part III of this article, Sawyer made a detailed analysis on why filtering technologies cannot accommodate fair use.

Foundation (EFF) also claims that filtering technologies can hardly accommodate fair use.[656] Therefore, technical filtering may result in over-filtering, and negatively affect the freedom of speech enjoyed by Internet users. In this regard, there seems a natural conflict between imposing a specific monitoring obligation and protecting Internet users' freedom of speech. Moreover, monitoring may also give rise to privacy concern. In the case of SABAM v. Scarlet, since the filtering system required by the SABAM would involve a systematic analysis of all content and the collection and identification of users' IP addresses from which unlawful content on the network was sent, the ECJ held such a filtering system was inappropriate and conflicted with privacy protection under the Charter of Fundamental Rights.[657]

Above all, in order to avoid an endless notice-and-takedown circle, obligations have been imposed on hosting ISPs to prevent repeated infringement. These obligations are justified under the terminology of "specific monitoring". Nevertheless, specific monitoring obligations can easily overstep the border with general monitoring obligations, and may impose unreasonable costs on hosting ISPs' operation. Further, based on the rationale embodied in "safe harbor" provisions, hosting ISPs' specific obligations should be defined by assessing their monitoring ability so as to avoid imposing unreasonable burden on them. However, this approach tends to result in legal uncertainty. Finally, specific monitoring may also conflict with Internet users' interests. Because of the drawbacks of imposing a specific monitoring obligation, this book proposes an alternative solution, and that is to treat specific monitoring as a reason to exempt hosting ISPs from liability rather than an obligation to make them liable. To be specific, if a hosting ISP does not implement specific monitoring, the court should not take it as a reason to hold the hosting ISPs liable. On the contrary, if a hosting ISP adopts specific monitoring, the court should treat it as a positive factor when deciding to grant the hosting ISP liability exemption.[658] This alternative solution avoids imposing unreasonable monitoring burdens on hosting ISPs, but still encourages hosting ISPs to implement specific monitoring against infringing materials.

4.7.3 Better Protection for the Highly Valuable Content

In China, hosting ISPs are obligated to undertake a higher duty of care on the specific content, including the content uploaded to the channel "movies and TV series," famous works and hot-playing audio-video works, and content being viewed

656 Fair Use Principles for User Generated Video Content, Electronic Frontier Foundation (n43).

657 *Scarlet Extended SA v SABAM* (n70), para. 26.

658 In the case of *Io Group, Inc. v. Veoh Internets, Inc.*, the court held the similar opinion. In this case, the defendant Veoh adopted filtering technologies to prevent the same infringing materials from being uploaded again, so the court took this effort as a reason to exempt Veoh from liability. See *Io Group, Inc. v. Veoh Internets, Inc.* (n5), at 1143.

over a certain number of times.[659] In fact, the higher duty of care as such is almost equal to monitoring duty, since if any of this content is successfully uploaded, the hosting ISP in question needs to be secondarily liable.[660] Some reasons can be drawn to support such a higher duty of care. First, these contents tend to be professionally created, and normally will not be made available to public without charge.[661] Second, since these contents are usually highly valuable, better protection of them can substantially reduce the damage caused to copyright owners. Third, although hosting ISPs cannot monitor all of the content uploaded by users, it is reasonable to limit the monitoring extent to these famous and high valuable ones.[662] Nevertheless, even though these reasons can to certain degree justify a better protection of these high valuable content, since these terms, such as "famous works," "hot-play movies and TV series," and "being viewed over a certain number of times," have not been well-defined by case law, legal certainty cannot be ensured. In this context, hosting ISPs tend to interpret these concepts in an amplified way, and thus monitor more content than necessary so as to avoid being held liable. In particular, it is really difficult to define "hot-play" and when a movie becomes not "hot-play" anymore, which may means hosting ISPs have to monitor a "hot-play" movie without time-limits. Therefore, without a proper explanation of several terms involved in a higher duty of care, hosting ISPs may have to introduce an unreasonably complicated and
148 costly monitoring system, which stifles their freedom to conduct business. In order to avoid unreasonably impeding hosting ISPs' freedom to conduct business, the Chinese courts should either clarify the limits of this highly valuable content or stop requiring hosting ISPs to undertake a higher level of duty of care to protect this content.

4.8 Conclusions

When deciding whether hosting ISPs are liable under the roof of "safe harbor" provisions, the courts in the US, EU and China evaluate some common factors, including no general monitoring obligation, the knowledge of infringement, measures against repeat infringement, benefit from infringement and inducement. Besides, Chinese courts require hosting ISPs to undertake a higher level of duty to protect highly valuable content. To be mentioned, with the development of Internet technologies, hosting ISPs adopt many new technologies to optimize their services, which substantially facilitate Internet users to share, locate and access information on the Internet. The facilitation as such not only helps Internet users access lawful information and useful knowledge, but also makes the access to infringing materials much easier. Especially, since there exist some hosting services

659 See what has been discussed in Section 4.6.
660 See the cases discussed in Section 4.6.
661 *nubb.com v. Tudou.com (新传在线v.土豆网)* (n591).
662 *Han Han v. Baidu (韩寒v. 百度)* (n42).

mainly used for infringing purposes.[663] In this situation, in order to protect better copyright owners' interests, the courts in the US, EU and China have relied more on the following factors to hold hosting ISPs liable, including intent (inducement), specific monitoring against repeat infringement and higher duty of care of highly valuable content. As discussed above, some strong arguments can be found to support these new liability criteria, but they need to be refined so as to avoid imposing an unreasonable burden on hosting ISPs. Regarding the intent of inducement, if a general intent of inducement can result in hosting ISPs' liability for the infringement committed by their subscribers, it may unreasonably restrict hosting ISPs' freedom to employ new technologies, and thus stifle the development of Internet technologies. With respect to specific monitoring against repeat infringement, it is better to not define specific monitoring as an obligation but rather treat it as a positive factor when deciding to grant hosting ISPs liability exemption. This approach avoids imposing an unreasonable monitoring burden on hosting ISPs, while encouraging them to implement specific monitoring. As for the higher duty of care on highly valuable content, since several terms used to define highly valuable content have not been clarified, hosting ISPs are exposed to legal uncertainty, which tends to force them to take more monitoring measures than necessary for their safety sake. Thus, such higher duty of care should not be imposed on hosting ISPs, unless the terms concerned are accurately defined.

The difficulty of regulating hosting ISPs' copyright liability actually reflects the overlaps and conflicts between different rights in respect of protecting intellectual property.[664] Too strong copyright protection may conflict with hosting ISPs' freedom of conducting their own business, and may even put Internet users' interests in danger.[665] In the US, EU and China, "safe harbor" provisions have been adopted to ensure hosting ISPs' freedom to operate, so the liability rules should not be interpreted in a way that impose an unreasonable burden on hosting ISPs. As also noted by Douglas Lichtman and William Landes, "Copyright law is important, but at some point copyright incentives must take a backseat to other societal interests, including an interest in promoting the development of new technologies and an interest in experimenting with new business opportunities and market structures."[666] This chapter explores how liability rules are interpreted under

663 See the Fung case, Rapidshare case and Newzbin case discussed above. The hosting services in these cases either aimed at promoting infringing use, or were widely used for infringing purpose.

664 Ruse-Khan HG, 'Overlaps and Conflict Norms in Human Rights Law: Approaches of European Courts to Address Intersections with Intellectual Property Rights' in Geiger C (eds), *Research Handbook on Human Rights and Intellectual Property* (Edward Elgar Publishing, 2015). As noted in this article, the conflicts between intellectual property protection and other rights have become quite frequent, which has aroused lots of discussion among academics.

665 See Lemley and Reese, 'Reducing digital copyright infringement without restricting innovation' (n3), at 1349. See also *SABAM v. Netlog* (n311), para. 44-46; *Scarlet Extended SA v SABAM* (n70), para. 26.

666 Lichtman and Landes, 'Indirect liability for copyright infringement: an economic perspective' (n12), at 401.

the roof of "safe harbor" provisions in the US, EU and China, and particularly examines these imputed factors that frequently result in hosting ISPs' liability according to the latest case law. Then, this chapter proposes on how these imputed factors ought to be interpreted so as to avoid imposing an unreasonable burden on hosting ISPs, which, the author believes, contributes to preserving maximum freedom for hosting ISPs to operate in the US, EU and China.

Chapter 5

Notice-and-takedown procedures in the US, the EU and China

Introduction:

According to the notice-and-takedown procedure, once a hosting ISP receives a proper complaining notice from copyright owner, it should promptly delete the infringing content indicated in the notification or block the access to the infringing content.[667] Notice-and-takedown procedure was firstly adopted by *DMCA* 512 in the US, and it can be seen as a creative way to cope with the overwhelming infringement on the Internet. Since a hosting ISP does not need to monitor the content uploaded by its users,[668] the notices from copyright owners work as a way to make a hosting ISP aware of the infringing content. Furthermore, notices of complaint can be sent in a large numbers, which fits in with the fight against an overwhelming level of infringing materials on the Internet, because hosting ISP can easily delete the infringing content by following the indications in the complaints. After *DMCA* 512 was enacted, the notice-and-takedown procedure has also been adopted by some other nations, and China is one of them. Although the EU has not introduced such a notice-and-takedown procedure into its *E-commerce Directive*, the Directive provides the basis for Member States to adopt this procedure.[669] In terms of Article 14(1)(b) of the *E-commerce Directive*, upon obtaining knowledge of any illegal information or activity, the hosting ISP needs to prevent access to the information expeditiously.[670] Therefore, after receiving such notices, which can result in hosting ISPs' knowledge of the infringement, they need to take down the
154 infringing materials. This chapter compares the notice-and-takedown procedures in the US, EU and China, and particularly analyses how the key issues ought to be interpreted in notice-and-takedown procedures so as to maximize hosting ISPs' freedom to operate in these jurisdictions.

Sections 5.1, 5.2 and 5.3 discuss the notice-and-takedown procedures in the US, EU and China, particularly examining how the courts in these jurisdictions apply notice-and-takedown procedures. In the US and China, notice-and-takedown is a statutory procedure, and the US and Chinese law includes the detailed provisions on regulating this procedure. But in the EU, notice-and-takedown procedure is mainly based on the fact that a notice might lead to ISPs' knowledge of infringement. Despite the existence of this basic difference, the courts in these three jurisdictional areas pay attention to similar problems while ruling on notice-and-takedown procedures, including to what extent should a notice demonstrate infringement, how exactly should a notice indicate the location of infringing materials, how to define "expeditiously remove", how to deal with the defect notices and the validity of ex ante notices. Section 5.4 compares how the courts in the US, EU and China deal with these common problems when interpreting notice-and-takedown procedures, and then answer how these common problems ought

667 DMCA (n1), Sec. 512 c(1)(c).
668 DMCA (n1), Sec. 512 m(1), E-commerce Directive (n1), Art. 15 of.
669 Commission Staff Working Paper: Online Services, Including E-commerce in the Single Market (n37), at 25.
670 E-commerce Directive (n1), Art. 14(1)(b).

to be solved. Further, although the notice-and-takedown procedure is an efficient tool to fight against overwhelming copyright infringement on the Internet, it also tends to result in wrong deletion. Section 5.5 explores the reasons resulting in wrong deletion, and then discusses hosting ISPs' duties in reducing wrong deletion. Finally, it summarizes the findings in previous sections, and then suggests how to cast hosting ISPs' duties in notice-and-takedown procedures and who should take the burden to reduce wrong deletion (5.6).

5.1 Notice-and-takedown Procedure in the US

As expected by the US Congress, notice-and-takedown procedure should function as the formalization and refinement of a cooperative process between ISPs and copyright owners which can be used to efficiently reduce copyright infringement on the Internet.[671] In order to ensure that this cooperative process will be widely adopted, an ISP cannot benefit from the liability limitation provided in "safe harbor" provision, if it refuses to take down the materials in question after receiving a qualified notification.[672] Meanwhile, copyright owners are also not obligated to send a complaint so as to enforce their rights, but if they do not send the qualified complaints, the limitation on liability will be applied, which means that actual knowledge or "red flag" knowledge of infringement still needs to be proved.[673] Since the notice-and-takedown procedure is so heavily reliant on reducing copyright infringement on the Internet, DMCA 512 includes some detailed provisions to regulate the operation of notice-and-takedown procedure,[674] which will be discussed in the following text.

5.1.1 Setting a Designated Agent

In order to ensure that the notifications can reach hosting ISPs properly, DMCA 512 requires the hosting ISPs to designate an agent particularly for receiving notifications from copyright owners.[675] Furthermore, a hosting ISP also needs to make the contact information of its agent publicly accessible, such as publishing the contact information in an obvious location of its website, and providing contact information to the Copyright Office for an index.[676] The contact information must include "the name, address, phone number, and electronic mail address of the agent" and "other contact information which the Register of Copyright may deem appropriate."[677] For the purpose of guaranteeing that copyright owners can find the contact information of agents, "the register of

671 H.R. REP. 105-551(II) (n16), at 54.
672 Ibid.
673 Ibid.
674 DMCA (n1), Sec. 512, (c)(2), (3), (f), (g)(3).
675 DMCA (n1), Sec. 512, (c)(2).
676 Ibid.
677 Ibid.

Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, in both electronic and hard copy format," and hosting ISPs may be required to pay the cost of maintaining the directory.[678]
Hosting ISPs need to keep their designated agents available to be contacted, which means if they change the contacts of the agents, they must promptly update the contact information and make the updating publicly accessible. In the case of *Ellison v. Robertson*, the defendant had changed the e-mail address to which infringement notifications were supposed to have been sent, and failed to provide for forwarding of messages sent to the old address or notification that the e-mail address was inactive, so the 9th Circuit Court concluded that the defendant did not fulfill the requirement of notice-and-takedown procedure for not having an effective notification procedure in place.[679]

5.1.2 Elements of Notification

In terms of notice-and-takedown procedure, a hosting ISP should remove the materials which are claimed to be illegal in a notification, so the notification must be competent and thus fulfill certain requirements. As provided in DMCA 512 (c)(3)(A), a competent notification should at least substantially include the following elements:[680]

(i) A physical or electronic signature of a person authorized to act on behalf of the
156 owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

678 Ibid.
679 *Ellison v. Robertson* (n402), at 1080.
680 DMCA (n1), Sec. 512, (c)(3)(A).

(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

After examining the elements listed above, one can find that DMCA set a very strict requirement on the content of notification. First, in order to ensure that a notification is sent with full caution, a competent notification should include the signature of an authorized sender, a statement of his good faith and the accuracy of notification. Second, a notification should include the identification of the copyrighted work claimed to be infringed and sufficient information about the alleged illegal material so that the receiver (hosting ISP) can easily locate the complained material without any further inspection. Third, in order to make sure that the complaining party can be contacted, a notification also needs to include the contact information of the complaining party. Finally, if a notification fails to substantially comply with these elements, it cannot be considered as evidence to decide whether the receiver (hosting ISP) has actual knowledge or "red flag" knowledge of infringement.[681] However, if a defective notification fulfills the elements (ii), (iii) and (iv) listed above, which raises enough suspicion to the receiver about the existence of infringement, the receiver shall notify the complaining party through the contact information given in the notification and assist the complaining party to perfect its notification.[682]

Among the elements required for notification, identification of the copyrighted works and identification of the infringing materials have been most frequently discussed during the hearings. Since the infringement always occurs in a large scale, copyright owners tend to send less concrete notifications to hosting ISPs so as to cover as much infringing material as possible. However, it seems that this kind of effort cannot always succeed. In the case of *Arista Records v. MP3Board*, the plaintiff sent three notifications to the defendant, and the first two letters merely listed a handful of performers whose works were claimed to be infringed.[683] Eventually, the court concluded the incompetence of these two letters because they neither accurately identified the copyrighted works nor infringing materials.[684] Nevertheless, the third letter was considered as competent, because it not only indicated the songs which were alleged to be infringed, but also included printouts of screenshots, on which 662 alleged infringing links were highlighted.[685] Furthermore, each notification must separately comply with the requirements, and the copyright owner cannot claim that the combination of several notifications, which are separately defective, is substantially competent. In the case of *Perfect 10 v. CCBill*, the

681 DMCA (n1), Sec. 512, (c)(3)(B)(i).
682 DMCA (n1), Sec. 512, (c)(3)(B)(ii).
683 *Arista Records, Inc. v. Mp3Board, Inc.*, 2002 WL 1997918, 9 (S.D.N.Y. 2002).
684 Ibid.
685 Ibid.

first two letters sent by the agent of plaintiff merely identified the copyrighted works being infringed and the infringing materials, but failed to declare, under penalty of perjury, that he was authorized to represent the copyright owner, and that he had good faith to believe that the complained materials were infringing. The third letter supplemented the declaration that was missing from the first two letters. The plaintiff tried to persuade the court to agree that the combination of the foresaid three notifications can be seen as one competent complaint. However, the court declined the plaintiff's effort and concluded that permitting a copyright holder to cobble together adequate notice from separately defective notices would unduly burden service providers.[686]

In order to best protect their interests, for certain high-valued contents, copyright owners may send notifications prior to the official issue of these contents.[687] However, the US courts refuse to admit the validity of these notifications. In the case of *Hendrickson v. Amazon.com*, the plaintiff, who owned the copyright to a movie, sent a notification to the defendant to claim that all DVD versions of the movie were infringing even before the DVD version was officially released, so actually the copyright owner sent a complaint when there was no material infringing his copyright on the defendant's website. Nevertheless, nine months later, the plaintiff found that the DVD version of his movie could be still found on sale on the defendant's website, so he claimed that the defendant should be liable because his notification leads to defendant's actual knowledge
158 of infringement. The court denied this claim, because the Congress thus intended the notice to make a service provider aware of infringing activity that is occurring at the time it receives the notice.[688]

5.1.3 Counter Notification

Since hosting ISPs need to promptly remove the materials which are the subject of a complaint upon receiving competent notification, in order to protect Internet users' right from being improperly eroded by false complaints, the notice-and-takedown procedure requires a hosting ISP to promptly notify the Internet users of removing or deleting their uploaded materials.[689] After receiving this notification from hosting ISPs, the Internet users can send counter notification to the hosting ISPs. The elements of counter notification are similar to those in notification, which are as follows: 1) a physical or electronic signature of the sender; 2) identifying the material which has been removed and indicating the location of the material as it appeared before; 3) a statement under penalty of perjury that the sender faithfully believes that the material was wrongly removed; 4) the sender's contact information, such as his name, address and telephone number, and also a statement about agreeing with the jurisdiction of Federal District

686 *Perfect 10, Inc. v. CCBill LLC*, 481 F.3d 751, at 761 (9th Cir, 2007).
687 See *Hendrickson v. Amazon.com, Inc.*, 298 F.Supp.2d 914, (C.D. Cal. 2003).
688 *Hendrickson v. Amazon.com, Inc.*, 298 F.Supp.2d 914, at 917 (C.D. Cal. 2003).
689 DMCA (n1), Sec. 512, (g)(2)(A).

Court in the US.[690]

Upon receiving the counter notification from an Internet user, the hosting ISP shall promptly forward a copy of counter notification to the person (copyright owner or his authorized agent) who sent the notification, and then informs that person that the removed material will be replaced in 10 business days.[691] Furthermore, the replacement must be done in no less than 10 but no more than 14 business days after receiving the counter notification; however, if the person who sent the notification has already notified the hosting ISP that he has sought a court order against the Internet user who sent the counter notification for his activity engaging in the infringement referred to in the notification, the hosting ISP did not need to perform the replacement.[692]

5.1.4 Limitation on Liability

After examining the operation of the notice-and-takedown procedure, one can find that during the whole process, hosting ISPs keep being passive and just follow the directions indicated by notifications and counter notifications. Therefore, DMCA 512 provides a wide liability limitation to these hosting ISPs who comply with the notice-and-takedown procedure. Even if the materials are wrongly removed or replaced, so long as hosting ISPs faithfully perform the removal and replacement pursuant to the notification and counter notification, they do not need to be responsible for any mistaken removal and replacement.[693]

5.1.5 Misrepresentations

As introduced in the last paragraph, hosting ISPs do not need to be responsible for wrong removal and replacement, so for their own good, they tend to follow the direction in notification or counter notification without examining whether the notification or counter notification is right or not. In order to prevent the notice-and-takedown procedure from being abused, DMCA provides that the person, who knowingly materially misrepresents whether the material or activity is infringing or not in his notification or counter notification, will be liable and pay for the damage incurred by his misrepresentation.[694] In this provision, the key point is how to interpret "knowingly materially misrepresent". In the case of *Online Policy Group v. Diebold*, the plaintiff sent a notification complaining about an e-mail archive of the corporate communications regarding the accuracy and security of the voting machines available on the defendant's website. The court concluded that the plaintiff knowingly materially misrepresented in its notification, because even if the archive of communication referred to above was

690 DMCA (n1), Sec. 512, (g)(3).
691 DMCA (n1), Sec. 512, (g)(2)(B).
692 DMCA (n1), Sec. 512, (g)(2)(C).
693 DMCA (n1), Sec. 512, (g)(2), (4).
694 DMCA (n1), Sec. 512, (f).

subject to copyright protection, they were clearly subject to the fair use exception.[695] Besides, the court also held that, in the context of DMCA 512(f), the "knowingly" meant that "a party actually knew, should have known if it acted with reasonable care or diligence, or would have had no substantial doubt had it been acting in good faith, that it was making misrepresentations."[696] As for the "materially", it means that "the misrepresentation affected the ISP's response to a DMCA letter."[697] Therefore, "misrepresentation" in DMCA 512 (f) is not easily proved. First, DMCA 512 (f) sets a quite high requirement on senders' subjective fault, and mere negligence cannot result in senders' knowingly misrepresenting. Second, the misrepresentation should lead to hosting ISPs' wrong deletion or removal of legal materials, which means that even though a complainant knowingly misrepresents in his notification, if the hosting ISP doesn't wrongly delete or remove the legal materials, the complainant needs not to be liable for his misrepresentation.

5.2 Notice-and-takedown Procedures in the EU

As mentioned at the beginning of this chapter, although the E-Commerce Directive does not include an explicit rule about any notice-and-takedown procedure, it does provide the basis for this procedure, since according to Article 14(1)(b), a notice leading to a hosting ISP's knowledge of infringement will trigger the hosting ISP's obligation to
160 taking down the infringement expeditiously. In the Member States, the courts also treat the notices from rights holders as an important factor when deciding on whether the hosting ISPs actually know of the infringement.[698] The European Commission has also recognized the importance of a notice-and-takedown procedure in respect of dealing with an overwhelming level of infringement on hosting platforms, and held a Public Consultation on Procedures for Notifying and Action on Illegal Content hosted by Online Intermediaries in 2012.[699] This public consultation demonstrated that there were huge disagreements over many key problems of notice-and-takedown procedure, such as the requirements for notices, how fast should remove be done, how to prevent unjustified notices, etc.[700] Nevertheless, so far no notice-and-takedown procedure has been harmonized at the EU level. Some Member States have adopted the codified

695 *Online Policy Group v. Diebold Inc.*, 337 F. Supp. 2d 1195, at 1204 (N.D.Cal. 2004).

696 Ibid.

697 Ibid.

698 Sadeghi, *The Knowledge Standard for ISP Copyright and Trademark Secondary Liability: A Comparative Study on the Analysis of US and EU Laws* (n368), at 105. See also Verbiest T et al., Study on the Liability of Internet Intermediaries (n389), at 36-46.

699 *A clean and open Internet: Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries*, European Commission(2012), *available at* http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-internet_en.htm (last visited 19-02-2014).

700 *Summary of Responses - A clean and open Internet: Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries*, European Commission(2012), *available at* http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-internet/summary-of-responses_en.pdf (last visited 04-05-2016).

notice-and-takedown procedures, including Finland, Hungary and Lithuania.[701] Some other Member States, such as France, Italy and the UK, have ruled on the elements of a competent notice in their national legislations about implementing the E-commerce Directive.[702] There are also Member States which have not even ruled on the elements of a competent notice at the legislative level, including Holland and Germany.[703] The following text explores how notice-and-takedown procedures are implemented in member states at both legislative and judicial levels under the roof of E-commerce Directive, including entity in charge of notice, formal requirement on notices, precise location of infringing materials, evidence about infringement and expeditious remove of infringing materials.

5.2.1 Entity in Charge of the Notice

In the EU, some Member States only acknowledge the notices from authorities at the legislative level, such as Spain and Italy.[704] In Spain, only notices sent by competent bodies, including a court or an administrative authority, can result in a hosting ISPs' knowledge of infringement from the legal perspective.[705] According to Article 16.1 (b) of the Spanish E-commerce law, a hosting ISPs shall be held to know the infringement, when "a competent body has declared the data to be illegal, has ordered its removal or that access to the data be blocked, or when it has been declared that the damage has been done, and the provider is aware of the relevant solution, without prejudice to the notice-and-takedown procedure that applies to the providers on the basis of voluntary agreements and of other effective knowledge-based means that can be established."[706] In 2012, Spain enacted Royal Decree 1889/2011 which appointed the Intellectual Property Commission as the competent body to deal with the notices from copyright owners, and then decide whether the takedown requests should be sent to the corresponding ISPs.[707] In Italy, the *E-Commerce Directive* has been implemented into *Legislative Decree 70/03*. According to Article 16.1 (b) of *Legislative Decree 70/03*, a hosting ISP, upon acquiring knowledge or awareness of infringement, or upon receiving a proper order from a court or a competent authority, should expeditiously remove or disable access to the infringing materials.[708] Therefore, the legislation in Italy only provides that a hosting ISP should take down infringing materials after receiving notice from competent authorities, but does not directly indicate whether a notice from private entities, such as copyright owners, can lead to the same effects.

701 Verbiest T et al., Study on the Liability of Internet Intermediaries (n389), at 106-109.
702 Szuskin L, et al., 'Beyond Counterfeiting: The Expanding Battle Against Online Piracy' (2009) 21 Intellectual Property & Technology Law Journal 4.
703 Verbiest T et al., Study on the Liability of Internet Intermediaries (n389), at 41-42.
704 Ibid, at 42.
705 Ibid.
706 Ibid.
707 Meliá JC, 'The Administrative and Judicial Procedure Concerning Internet Infringements: Much More Than a Simple Notice and Takedown Procedure' (2014), WIPO/ACE/9/21.
708 Legislative Decree 70/03, Art. 16.1 (b), quoting Bellan, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in Italy' (n238), at 90.

Although competent authorities can send hosting ISPs notices which result in the accurate removal of infringing materials, authorities are incapable of pursuing every infringement because of the limited resources they have.[709] Further, in the case of *L'Oréal SA v. Ebay*, the ECJ held that hosting ISPs' knowledge of infringement can be acquired through either their own investigation or private notices.[710] Therefore, member states also acknowledge the effectiveness of notices from private entities, so long as these notices can result in hosting ISPs' knowledge of infringement. For example, Finnish law acknowledges that both a court order and a competent notice from copyright owners can trigger hosting ISPs' obligation to take down infringing materials.[711]

5.2.2 Formal Requirement on Notices

Regarding the notices sent by competent authorities, the relevant legislation in the member states does not set formal requirements on them, since the accuracy of these notices can normally be guaranteed.[712] However, regarding the notices from copyright owners, several member states prescribe the elements of a competent notice at legislative level so as to make notice-and-takedown procedure work properly.

As provided by Finnish law, a competent notice should include the following elements: 1) details of the notifying party, 2) material in itemised form, 3) location of material, 4) confirmation that material is illegally accessible, 5) information that notifying party
162 has in vain contacted content provider, 6) confirmation that notifying party is copyright holder.[713] Although the UK and France do not adopt a codified notice-and-takedown procedure, they do rule on the elements of notice. In the UK, a notice must include the following elements: "1) the full name and address of the sender of the notice; 2) details of the location of the information in question; and 3) details of the unlawful nature of the activity or information in question."[714] France even drafts a detailed list of elements, comparable to those in Finnish law regarding notice. As provided in *LCEN* (Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique), a notice should include:[715]

709 Verbiest T et al., Study on the Liability of Internet Intermediaries (n389), at 15.

710 *L'Oréal SA and Others v eBay International AG and Others* (n327), Para. 122.

711 Fahllund K, *Country Report (Finland)*, Global Advertising Lawyers Alliance(2002), *available at* http://www.gala-marketlaw.com/pdf/finland2002.pdf (last visited 20-08-2014).

712 In Finland, Italy and Spain, where notices from authorities are acknowledged, legislation has not set formal requirement on the element of notices. See Commission Staff Working Paper: Online Services, Including E-commerce in the Single Market (n37), Annex II. Fahllund, Country Report (Finland) (n706). Bellan, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in Italy' (n238), at 91-92.

713 Commission Staff Working Paper: Online Services, Including E-commerce in the Single Market (n37), Annex II.

714 Electronic Commerce (EC Directive) Regulations 2002 (n155), Art. 22 (b).

715 LCEN (n171), Art. 6-I-5.

□ 1) The date of notification;
□□ 2) The identity of the person who sends notice. If the sender is a natural person, the notice should indicate his/her full name, occupation, residence, nationality, date and place of birth. If the sender is a legal entity, the notice should indicate its legal form, its name, registered office, and legal representative;
□□ 3) The name and address of the recipient. If the recipient is a legal entity, the notice should indicate its name and headquarters;
□□ 4) The description of the alleged infringing materials and their precise location;
□□ 5) The reasons for which the content should be removed, including the reference to legal provisions and justification of the claims;
□□ 6) A copy of correspondence between the sender and the author or publisher of the disputed materials, which requires that the disputed materials should be removed. If no copy of correspondence can be offered, the notice should state the reasons why the author or publisher could not be contacted.

Although the member states discussed above have already ruled on what elements should be included in a competent notice, in judicial practice there still exist disputes on how to interpret some of these elements. In the member states where no norm regulates the elements of notices at legislative level, similar disputes also exist on what constitutes a competent notice. Generally, the disputes focus on how to interpret "the precise location of alleged infringing materials" and "the evidence to prove the illegality of alleged infringing materials."[716] The following section explores how these two elements are interpreted in several member states.

163

5.2.3 Precise Location of Alleged Infringing Materials

Since hosting ISPs are not obliged to actively seek infringing materials on their platforms,[717] in order to make them aware of infringing materials, notices should include the precise location of alleged infringing materials. Regarding how precise the location ought to be indicated, the courts in member states deliver different decisions.

In the case of *Nord-Ouest v. Dailymotion*, the Court de Cassation (French Supreme Court) held that the information about the location of infringing materials in a notice had to be sufficient for the ISP to identify them, and the simple mention of a video available on the ISP's website was not enough.[718] In Germany, in the case of *GEMA v. YouTube*, the plaintiff GEMA is a collecting society for musical performance and mechanical reproduction rights based in Germany, and it sent a notice to the defendant YouTube to complain that 258 music works managed by it were made unlawfully

716 Commission Staff Working Paper: Online Services, Including E-commerce in the Single Market (n37), at 43.
717 E-commerce Directive (n1), Art. 15.
718 Bellan, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in Italy' (n238), at 72.

accessible on the YouTube.[719] Afterwards, the plaintiff sued YouTube for copyright infringement, since some of music works were still publicly accessible. In these notices, not only the titles and the authors of music works were indicated, but also the URLs of infringing videos were given.[720] Therefore, the Hamburg District Court concluded that the notices sent by plaintiff were competent, since it was quite easy for the defendant to locate the infringing videos by following the URLs given in the notices, and the defendant should immediately remove the infringing videos.[721] Further, in Germany, besides URLs, some other indications can also precisely help hosting ISPs locate the alleged infringing materials. In the case of *Stiftparfuem*[722]*, Federal Supreme Court held the plaintiff pointed out that all of the perfumes branded in "Echo Davidoff" and "Davidoff Cool Water Deep" in capacity of 20 ml were counterfeits without exception, so the defendant did not need to examine the likelihood of confusion, but just identify the perfumes in the same trademark and capacity.*[723] *Therefore, in the notice, the plaintiff indicated all the legal and factual circumstances, from which the infringement could be clearly and easily identified by the defendant, since the defendant could locate all of the infringing offers by searching with the keywords of trademarks, capacity and product categories on its auction platform.*[724]

In Italy, different courts even delivered contradicting opinions. In a series of cases between RTI and YouTube, IOL, Yahoo!, the Plaintiff, as copyright owner, sent notices that only identified the titles of the TV programs being illegally uploaded but did not include the
164 URLs of infringing materials, to the defendants. Finally, the court held that this kind of notices were competent, since although the URLs of alleged infringing materials were not provided, the platforms operated by the defendants offered internal search engines through which the defendants could easily identify the infringing materials by inputting the titles of the TV programs as searching key words.[725] By following the same approach, the District Court of Roma further stated that "it would be unreasonable to burden RTI with the additional work of providing Google with the URLs for any single infringing video."[726] However, in another case with nearly the same facts, the District Court of Turin held an opposite opinion. In the case of *Delta TV v. YouTube*, the plaintiff Delta TV found that some episodes of its copyrighted TV series could be accessed on the YouTube, and then Delta TV sent YouTube a notice which only indicated the titles of the

719 LG Hamburg, Urteil vom 20.04.2012, 310 O 461/10.

720 Ibid.

721 Ibid.

722 It is a case about trademark infringement on hosting platforms, but because German courts did not differentiate between the notice-and-takedown procedures applied to copyright infringement and trademark infringement, this case can be mentioned to demonstrate how German courts interpret "the precise location of alleged infringing materials."

723 BGH, August 17, 2011, Case No. I ZR 57/09 - *Stiftparfuem*, para. 29.

724 Ibid, para. 29.

725 Bellan, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in Italy' (n238), at 112.

726 Bellan, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in Italy' (n238), at 112-113.

videos alleged as infringing. Based on these facts, the District Court of Turin concluded that the notice sent by the Delta TV could not lead to the defendant's actual knowledge of complained infringement, since it did not indicate the URLs of the infringing videos, which could not make the defendant accurately identify the alleged infringement.[727] Therefore, according to District Court of Turin, it is necessary for a competent notice to include the exact URLs of infringing materials. Based on the case law discussed above, it can be concluded that a notice including the URLs of alleged infringing materials can definitely meet the requirement of precisely indicating the location. However, whether other indications, such as titles of works, authors of works, names of albums, etc., can precisely indicate the location of alleged infringing materials remains uncertain in Member States.

5.2.4 Evidence to Prove the Illegality of Alleged Infringing Materials

Because the actual knowledge or awareness in Article 14 of E-commerce Directive covers not only the suspected materials, but also their illegality,[728] notices are supposed to include sufficient evidence to prove the illegality of suspected materials so as to trigger the hosting ISPs' duty to take them down. Regarding what constitutes sufficient evidence in a notice, the courts in different member states deliver different decisions.

In Germany, the case of "Stiftparfuem" provides us a good insight into this issue. In this case, the plaintiff sent a notice to the defendant Ebay, and alleged that all of the perfume "Echo" and "Cool Water Deep" in capacity of 20 ml sold on Ebay were counterfeits. However, the Higher Regional Court of Düsseldorf held this notice incompetent. First, the Court held that, from the perspective of the defendant, it's highly possible for the plaintiff to produce and distribute the perfumes on the market, since it is quite common for perfume manufacturers to sell the perfume in a capacity of 20 ml on the market.[729] Therefore, it is the plaintiff's duty to prove its claim that it had not produced the complained perfumes in a capacity of 20 ml, but it failed to do so. Second, the notice also did not make it clear that the plaintiff had rights to pursue the infringement.[730] Third, the evidence offered by the plaintiff was insufficient to arouse the defendant's duty to check out the alleged infringement, since the plaintiff only made a general statement that the complained perfumes were counterfeits. Besides, the notice did not show the corresponding original perfumes so that the fake nature of the offers could not be clearly and unambiguously recognizable. Therefore, for an objective viewer, it was possible that the designated perfumes were genuine.[731] By deducing from the conclusion made by

727 Spedicato, 'Italy: the take-down notice must contain the specific YouTube URLs' (n437).
728 E-commerce Directive (n1), Art. 14.
729 OLG Düsseldorf, Urteil vom 31.03.2009, I-20 U 73/08.
730 Ibid.
731 Ibid.

the Higher Regional Court of Düsseldorf, a competent notice should include sufficient evidence which could substantially prove that the offers were counterfeits.

The German Federal Supreme Court, however, came to a different conclusion in this aspect.[732] The Germany Federal Supreme Court differentiated between the indication about a specific infringement and the evidence to justify the legality of that indication.[733] The indication was sufficient to arouse the defendant's duty to remove the complained offers. However, the evidence was only needed when the defendant had reasonable doubts about the legality of the indication. For instance, the defendant had reasonable doubts on the existence of a property right, the authorization to enforce this property right or the truth of the reported facts about an infringement; it therefore needed to undertake a costly investigation so as to surely identify the infringement.[734] In this case, the defendant could have reasonable doubts on whether the products mentioned in the complaint infringed the plaintiff's right, and whether the plaintiff was authorized to enforce this right.[735] However, once having reasonable doubts, the defendant was obliged to notify the plaintiff of these doubts and ask the plaintiff to provide relevant evidence to clarify these doubts, but it failed to do so.[736]

Above all, in the view of the German courts, normally, a notice which includes the clear indications about a specific infringement can trigger the hosting ISP's removing duty; however, if the hosting ISP has reasonable doubts about the legality of the indication, it
166 is obligated to ask the sender to provide the relevant evidence to justify that indication.

In the UK, the courts seem to set a stricter requirement on the evidence included in notices. In the case of *Bunt v. Tilley*, the Queen's Bench Division held that "in order to be able to characterize something as 'unlawful' a person would need to know something of the strength or weakness of available defense."[737] Therefore, unless the sender has clarified why any potential defenses would not apply in a notice, the ISP should not be held as having actual knowledge of the unlawful activity under the Regulation.[738] By following the Interpretation about "details of the unlawful nature" in *Bunt v. Tilley*, a copyright notice needs to not only include evidence about infringement, but also demonstrates why the defense, such as fair use, is not applicable.

Since notices should include evidence about infringement, hosting ISPs need to evaluate this evidence so as to decide whether the designated materials are infringing. In Germany, upon receiving a notice, the hosting ISP at least needs to conduct a preliminary assessment on the evidence in the notice so as to see whether there exists any

732 BGH – *Stiftparfuem* (n718).
733 Ibid, para. 31.
734 Ibid, para. 31.
735 Ibid, para. 32.
736 BGH – *Stiftparfuem* (n718), para 32.
737 *Bunt v Tilley and others*, [2006] EWHC 407 (QB), para. 72.
738 Smith GJH and Boardman R, *Internet Law and Regulation* (Sweet & Maxwell. 2007), at 379.

reasonable doubt on the truth of the reported infringement.[739] In order to avoid imposing too much burden on a hosting ISP who had received notices, the German Federal Supreme Court stated that the action of hosting ISPs was only initiated, if the notices were so concretely drafted that the infringements alleged by the senders could easily be identified, i.e. without complicated legal and factual inspection.[740] Besides, how much inspection is required to be done by a hosting ISP depends on the circumstances in each case, especially, the gravity of the alleged infringement on the one hand, and the hosting ISP's possibility of knowledge on the other hand.[741] In France, in order to relieve hosting ISPs' assessing burden, the French Constitutional Council held, only when materials are manifestly unlawful or the court issues an order to remove, need hosting ISPs expeditiously remove the materials at issue.[742] Therefore, by following this jurisprudence, only the notices which complain about manifestly unlawful materials can arouse the hosting ISPs' obligation to remove the alleged infringing materials. Regarding what constitute "manifestly unlawful" materials, the French Constitutional Council did not specify more on this notion.[743] One French court had held, "the sale of copyrighted video games well below under the counter price constitutes such a manifest infringement."[744]

Hosting ISPs' assessment on infringing evidence in notices arouses lots of criticism in the EU. First, unlike the child pornography which is manifestly unlawful, to conclude a copyright infringement is far more complicated, and hosting ISPs may not be capable of reaching the right decisions.[745] Further, the assessment on infringing evidence forces hosting ISPs to act as private judges, and some people argue that it is not legitimate and feasible for hosting ISPs to assess the illegality of the materials which are the subject of a complaint.[746]

5.2.5 Expeditiously Remove Infringing Materials

If the materials turn out to be infringing according to hosting ISPs' assessment, hosting ISPs need to expeditiously remove these infringing materials.[747] Regarding what constitutes expeditiously removing, some codified notice-and-takedown procedures provide the specific timeframes for hosting ISPs to carry out removal.[748] In Hungary,

739 BGH – Stiftparfuem (n718), para. 31.
740 Ibid.
741 BGH: Verantwortlichkeit des Host-Providers für Persönlichkeitsrechtsverletzung durch Blog-Eintrag, GRUR 2012, 311, para. 26.
742 Jasserand C, *France- Dailymotion heavily fined for the late removal of infringing content*, wolters kluwer law & business(2012), *available at* http://kluwercopyrightblog.com/2012/09/28/france-dailymotion-heavily-fined-for-the-late-removal-of-infringing-content/, (last visited 28-09-2014).
743 Ibid.
744 Verbiest T et al., Study on the Liability of Internet Intermediaries (n389), at 39.
745 Ibid, at 36.
746 Commission Staff Working Paper: Online Services, Including E-commerce in the Single Market (n37), at 45.
747 E-commerce Directive (n1), Art. 14.1 (b).
748 Commission Staff Working Paper: Online Services, Including E-commerce in the Single Market (n37), at 44.

with regard to intellectual property infringement, hosting ISPs need to act within 12 hours after receiving notices.[749] In Lithuania, hosting ISPs have to act within 1 day upon receiving notices complaining of copyright infringement.[750] Nevertheless, most member states in the EU have not set a timeframe for hosting ISPs to conduct removing, so what constitutes expeditiously removing is mainly left for courts to decide according to the concrete facts in individual cases.[751] For example, in France, in the case of TF1 v. YouTube, the Court of First Instance in Paris held that it was unreasonable for YouTube to remove the alleged infringing materials 5 days after receiving the notice from the plaintiff.[752] In another case, the defendant Daily motion removed the alleged infringing materials 4 days after receiving notice, and the same court held that it was too long.[753] In the case of SPPF v. YouTube, the court held that removing the infringing material in 2 days was reasonable.[754]

5.2.6 Other Issues about Notice-and-takedown Procedures

According to notice-and-takedown procedures, the alleged infringing materials can be removed without judicial review, so it is possible that materials are wrongly removed. Therefore, the notice-and-takedown procedure codified in DMCA provides a counter for Internet users to retrieve their materials which are wrongly removed.[755] In the EU, the counter-notice procedures exist in the Member States where the notice-and-takedown procedures have been adopted at legislative level, including Finland, Hungary and
168 Lithuania.[756] For instance, in Finland, if Internet users believe that the removal of their materials is groundless, they can send counter notices to ISPs in 14 days after receiving notices so as to have their materials restored.[757] In the Member States which have not codified notice-and-takedown procedures, there exists no counter-notice procedure.

749 Ibid.
750 Ibid.
751 Ibid, at 44-45.
752 Jasserand C, *France -Youtube guilty but not liable? some more precisions on the status of hosting providers*, wolters kluwer law & business(2012), *available at* http://kluwercopyrightblog.com/2012/06/18/france-youtube-guilty-but-not-liable-some-more-precisions-on-the-status-of-hosting-providers/, (last visited 28-09-2014).
753 Jasserand, *France- Dailymotion heavily fined for the late removal of infringing content* (n742).
754 Leger P, *Internet Service Providers' liability in France*, CERDI(2012), *available at* https://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0CCwQFjAC&url=http%3A%2F%2Fwww.cerdi.u-psud.fr%2Fwp-content%2Fuploads%2F2013%2F05%2FInternet-service-providersliability-in-France-P-Leger.pptx&ei=K33eVKi1J4SfPayYgPAM&usg=AFQjCNGmn-YXh1IrydyS1MoV8I51HEwRVQ&sig2=wSi5ADRPXJh7jgnS1I0yeQ&bvm=bv.85970519,d.d2s (Last visited 12-08-2014).
755 DMCA (n1), Sec. 512, (g)(2),(3).
756 Verbiest T et al., Study on the Liability of Internet Intermediaries (n389), at 106-109.
757 Ibid, at 106.

Regarding who should be liable for the wrong removal, it is normally held that hosting ISPs are exempted from liability if they commit the removing by following the claims in the notices.[758] As for notifiers who send the wrong notices, the legislation in some member states declares that if they send notice in bad faith, they should be liable. For instance, in Finland, if a notifier delivers false information in a notice, he needs to be liable for the damage resulting from that false information.[759] However, if the notifier has reasons to believe the false information offered by him is correct, he should not be held liable.[760] In France, in order to avoid the abuse of notice-and-takedown procedure, the LCEN provides that if a person sends a notice to an ISP with knowledge of its inaccuracy, he would be sentenced to prison for 1 year and fined 15 000 euros.[761]

Based on the above discussion about notice-and-takedown procedures in the EU, it is not difficult to find out that because of no harmonization at the EU level, the regulation of this procedure in the EU turns out to be fragmented. Some member states provide the codified notice-and-takedown procedures, including Finland, Hungary and Lithuania. Some member states prescribe the elements of a competent notice in their legislation, including France and the UK. Some member states only recognize the effectiveness of notices sent by competent authorities at legislative level, including Spain and Italy. Some member states have not ruled on notice-and-takedown procedure in their legislation at all, including the Netherlands and Germany. Despite the existence of these differences in the EU, the case law in member states deals with some common problems when regulating notice-and-takedown procedures, including how exactly should the location of infringing materials be indicated (including URLs or not), to what extent should the unlawful nature of materials be demonstrated, in how many days should an ISP remove the materials after receiving notice.

5.3 Notice-and-takedown Procedure in China

Even before China officially adopted "safe harbor" provisions in Internet Regulation, the Chinese Supreme Court had already provided a notice-and-takedown procedure in Internet Interpretation (2000). If looking into the notice-and-takedown procedure adopted by the Internet Interpretation (2000), it can be found that the Supreme Court took DMCA 512 as an important reference. According to this Interpretation, a hosting ISP needs to take measures to eliminate infringement after receiving an evidential warning notice from copyright owners, and otherwise it shall undertake liability for

758 According to the codified notice-and-takedown procedures in Finland, Hungary and Lithuania, ISPs do not need to be liable for wrong removing, if they follow the instruction in notices. See ibid, at 106-109. Besides, according to a Commission Staff Working Document, if ISPs respect notice-and-takedown procedures, even though the removed materials finally turn out to be not illegal, they need not to be liable. See also Commission Staff Working Paper: Online Services, Including E-commerce in the Single Market (n37), at 45.

759 Fahllund, Country Report (Finland) (n706).

760 Ibid.

761 LCEN (n171), Art. 6-I-4.

infringement.[762] Furthermore, the Internet Interpretation (2000) also rules on elements of a notice, and according to it, a competent notice needs to at least include the proof of sender's own identity, the proof of his copyright ownership and the proof about the infringement.[763] Finally, the Internet Interpretation (2000) exempts hosting ISPs from liability if they follow the competent notices, and copyright owners shall be responsible for the damage caused by their wrong notices.[764] However, the Internet Interpretation (2000) did not copy every part of the notice-and-takedown procedure from DMCA 512; for example, it does not grant service subscribers the right to send counter notices. In addition, the notice-and-takedown procedure provided in the Internet Interpretation (2000) is far less detailed than that in the DMCA. Therefore, the simplified notice-and-takedown procedure drafted by the Supreme Court left too much room for the lower courts to interpret, which leads to legal uncertainty in judicial practice. After several years, the State Council of China promulgated the Internet Regulations which include a detailed notice-and-takedown procedure. The Internet Regulations provide the elements of a competent notice, the effectiveness of a competent notice, the elements of a competent counter notice and the liability of wrong deletion in Article 14, Article 15, Article 16 and Article 24 respectively.

170

> Article 14: the notice should consists of at least the following contents: (1) the name, contact information and address of the copyright owner; (2) the titles and web addresses of the alleged infringing works, performances, sound recordings and audio-visual products (hereinafter collectively referred to as the "materials") which are required to be deleted or whose links are to be cut; and (3) the preliminary evidence for proving infringement.[765]

> Article 15: after receiving a notice from the copyright owner, the ISP shall immediately remove the material suspected of infringement or disable access to the link to the material suspected of infringement, and shall simultaneously forward the notice to the service recipients who transmit the material.[766] Furthermore, where the web address of a service recipient is not clear and therefore the forwarding is impossible, the notice contents shall be simultaneously announced on the internet.[767]

> Article 16: if the service recipient, who receives the notice about deletion from the ISP, deems that the deleted content doesn't infringe any other's copyright, it may file a written counter-notice to request of restoring the deleted content, and the counter-notice should contain the following elements: (1) the name (title), contact information and address of the service recipient; (2) the names of the works, performance, audio recordings and audio-visual products as well as web

762 Internet Interpretation (2000) (网络解释（2000）) (n190), Art. 5.
763 Ibid, Art. 6 and Art. 7.
764 Ibid, Art. 8.
765 Internet Regulations (网络条例) (n1), Art. 14.
766 Ibid, Art. 15.
767 Ibid.

addresses requested for recovery; and (3) the preliminary evidential materials for proving non-infringement.[768]

Article 17: after receiving a written statement from a service recipient, the ISP shall immediately replace the deleted works, performances, audio recordings and audio-visual products or recover the link to the aforesaid materials, and shall simultaneously transfer the written statement of the service recipient to the relevant copyright owner, and then the copyright owner cannot request the ISP to delete materials which has been recovered or to cut off the relevant link anymore.[769]

Article 24: if the relevant ISP, as a result of the copyright owner's notice, wrongly removes the material or disables access to the link to the material and therefore causes any damage to its service recipient, the copyright owner shall be subject to compensation.[770]

From the introduction mentioned above, it seems that the notice-and-takedown procedure in China has been well-established, since every stakeholder can defend its legal interests in this procedure. However, the Internet Regulations also include some blurred terms, such as "preliminary evidence", which are quite confusing. In practice, what constitutes "preliminary evidence" aroused lots of discussion about how much evidence is sufficient for a competent notice. Some commentators understand the "preliminary evidence" as prima facie evidence, which means that the notice should contain sufficient evidence to prove the existence of infringement, not only including the evidence about ownership but also infringing evidence which requires the comparative analysis of the copyrighted work and the infringing material.[771] It seems that this opinion is adopted by the National Copyright Administration of China (NCAC). In a model form of notice published by the NCAC, it is clearly indicated that evidential materials in a competent notice should include the physical evidence and documentary evidence of infringement, and the certification of copyright ownership.[772] However, if we interpret the "preliminary evidence" in such a strict sense, there would be at least two problems. First, on the Internet, copyright infringement always occurs on a large scale; if copyright owners are required to offer prima facie evidence in each notice, it would be too burdensome for them and go against the initial purpose of setting a notice-and-takedown procedure which aims at providing an efficient way to remove the infringing materials. Second, it would be also a burdensome work for hosting ISPs to examine the notices if prima facie

768 Ibid, Art. 16.
769 Ibid, Art. 17.
770 Ibid, Art. 24.
771 See Liu JR (刘家瑞), 'ISP Safe Harbours in China (论我国网络服务商的避风港规则--兼评"十一大唱片公司诉雅虎案")' (2009), 19 Intellectual Property (知识产权) 13, at 19.
772 Instruction about How to Fill in "the Notice requiring the deletion of or cutting off the links to infringing materials" (《要求删除或断开链接侵权网络内容的通知》填写说明), http://www.ncac.gov.cn/chinacopyright/contents/574/20879.html, (last visited 14-11-2014).

evidence is required to be included in the notices, and also would force hosting ISPs to perform like judges rather than intermediaries between copyright owners and service recipients.

Based on the reasons stated above, some Chinese courts have already lowered the copyright owners' burden of proving infringement in their notices. In the case of *Miao Fuhua v. 56.com*, the plaintiff Miao Fuhua owned copyright of a video product called "QuJuMingChouLiTianFang", and after she found that this video product was illegally uploaded to 56.com, she sent a notice to the 56.com and required the infringing video to be immediately deleted. Even though the notice sent by the plaintiff only indicated the information of copyright owner, the name of the video product being infringed and the certificate of ownership, the Beijing Chaoyang District Court still held that the notice was competent.[773] Therefore, according to Chaoyang District Court, copyright owners only need to offer the certificate of ownership and the video suspected to be infringing as preliminary evidence.

Further, in China, a competent notice needs to indicate the location of infringing material so that hosting ISP can easily find the suspected infringing material. The provision in the Internet Regulations appears quite clear, which requires copyright owners to offer the web address of infringing material in the notices.[774] In the case of *Fanya E-commerce v. Baidu.com*, the plaintiff Fanya, as a copyright owner of music works, sent notices to the
172 defendant Baidu.com to complain about the links pointing to illegal copies of its music. The notices sent by the plaintiff can be divided into two groups, one of which included the names, lyrics and authors of the music, and also the web address of infringing links, but the others missed the web address of infringing links. Finally, the Beijing Higher Court held that the second group of notices was not competent, since it would be too burdensome for the defendant to find the infringing links merely by referring to the names, lyrics and authors of the music.[775]

However, not all courts hold that the concrete web address is necessary for a competent notice. In the case of "*Universal Music v. Yahoo.cn*", the Universal Music, as the plaintiff, sent two notices to the defendant Yahoo.cn to complain about the links to infringing materials. The notices indicated the names of singers and albums, some URLs of infringing links and also attached the screenshot of these infringing links. But for each music work alleged to be infringed, the notices only offered one URL of many infringing links, and the plaintiff called it the infringing sample. Nevertheless, the plaintiff required

773 *Miao Fuhua v. 56.com (苗富华诉北京我乐信息科技有限公司等侵犯著作权纠纷案)*, Beijing Chaoyang District Court (北京市朝阳区人民法院), Chao Min Chu Zi No.30077 ((2011)朝民初字第30077号).

774 Internet Regulations (网络条例) (n1), Art. 14.

775 *Fanya E-commerce v. Baidu.com (泛亚电子诉百度侵权信息网络传播权案)*, Beijing Higher Court (北京市高级人民法院), GaoMinChuZi No. 1201 ((2007) 高民初字第1201号). Actually, this is case is about an ISP who runs a search engine, but since hosting ISPs and ISPs who run search engines are covered by the same notice and takedown regime, this case still can be used as a reference to indicate how Chinese courts interpret competent notices.

the defendant to disable access to all of the infringing links to its music by referring to the names of the singers and albums, and claimed that all the music links that were directed to these singers and albums were infringing. The defendant, however, merely disabled access to the links where the URLs were given in the notices, so the plaintiff asked the Court to hold the defendant secondarily liable for the infringement. Eventually, the Second Intermediate Court of Beijing held that after receiving the notices, the defendant has already got the information about the music being infringed, and should know that the infringing links to the plaintiff's music can be identified through its music searching engine; but the defendant merely cut off the infringing links that these URLs were given and failed to cut off the other infringing links, so it had subjective fault for the continuity of infringement and should be jointly and severally liable.[776] Therefore, according to the Second Intermediate Court of Beijing, it is unnecessary for a competent notice to include the URLs of all infringing materials.

Recently, the Chinese courts pay more attention to whether a notice can make ISPs accurately locate the infringing materials rather than whether a notice provides the URLs of infringing websites. In terms of Guiding Opinions published by the Beijing Higher Court, if a notice submitted by a copyright owner does not include the URLs of infringing materials, but offers sufficient information for an ISP to accurately locate the infringing materials, this notice can be concluded as competent.[777] As for whether the infringing material can be accurately located, the following factors should be comprehensively considered: the service offered by ISPs, the types of works (literature, performance, audio recording, or audio-video product) required to be removed or their links disabled, and whether the names of these works are specific or not.[778] Under the notice-and-takedown procedure, a competent notice is supposed to indicate the accurate location of infringing material being complained about, and then the ISP can take it down; so in this regard, the standard of "accurately locate" seems quite proper. However, notice-and-takedown procedure also needs to take the efficiency into account. Sometimes an ISP can accurately locate the infringing materials by following the information offered in the notice, but it might take too much time to do so. Therefore, the standard of "accurately locate" has its own weakness, and that might be why Internet Provisions (the latest Judicial Interpretation) does not include this standard in its final version.[779]

Regarding what constitutes "immediately remove" after receiving notices, there is no common standard being reached in practice. In the case of *Ningbo Success Multi-media Telecom v. Yahoo.cn*, the plaintiff "Ningbo Success Multi-media Telecom" owned the

776 *Universal Music v. Yahoo.cn (环球唱片诉雅虎侵犯信息网络传播权案)*, Beijing Second Intermediate Court (北京市第二中级人民法院), ErZhongMinChuZi No. 02622 ((2007)二中民初字第02622号).

777 Guiding Opinions (指导意见) (n229), Art. 28.

778 Ibid, Art. 29.

779 Internet Provisions (网络规定) (n208). The drafted version incorporated "accurately locate" standard in Art. 17, but it was deleted in the final version.

copyright of a TV series named as "Fendou (Combat)", and in the platform operated by the defendant Yahoo.cn, the plaintiff found that there were some links directing to the websites from which its TV series could be watched without permission. Later, the plaintiff sent a notice to the defendant, and the defendant removed the infringing links on the day of receiving the notice. Finally, the Chaoyang District Court (Beijing) held that the defendant fulfilled its obligation to immediately remove the infringing links.[780] In another case that has been discussed before (*Universal Music v. Yahoo.cn*), the plaintiff required Yahoo.cn to remove the infringing links in 7 days after receiving the notice.[781] As the biggest literature-sharing platform in China, BaiDuWenKu has a policy that the alleged infringing contents will be removed in 48 hours after receiving competent notices.[782]

It should be noted that the Guiding Opinions of the Beijing Higher Court do not set a fixed term for deciding whether a removal is immediate or not, but indicates some factors to be comprehensively considered, and they are as follows: the way of sending the notice, the accuracy of notice, the amount of infringing documents indicated by the notice, how hard it is to remove the materials or disable access to links, the characteristics of internet service, and other relevant factors.[783] Furthermore, the Supreme Court had tried to set a fixed term for ISPs to remove the materials or disable access to links. According to the draft of Internet provisions, except having reasonable excuse, the ISPs should take necessary measures against infringing materials in a working day after
174 receiving competent notice if the notice complains about illegal transmission of hot-play[784] movies or TV series, but for the other types of work, ISPs should take necessary measures in no more than 5 working days.[785] However, in the final version of the Internet Provisions, this Article has been deleted, and like the Guiding Opinions of Beijing Higher Court, the Internet Provisions only enumerate some factors for courts to evaluate. These factors are as follows: the way of sending notice, the accuracy of notice, how hard it is to take measures, the characteristics of Internet service, and the types, fame, amount of works, performance, sound recordings and audio-video products being infringed.[786] In consequence, the Supreme Court adopts a similar approach to that taken by the Beijing Higher Court, and leaves more flexibility for lower courts to interpret "immediately remove" based on the concrete facts in each case.

780 *Ningbo Success Multi-media Telecom v. Yahoo.cn (宁波成功多媒体诉雅虎侵犯著作权纠纷案)*, Beijing Chaoyang District Court (北京市朝阳区人民法院), Chao Min Chu Zi No. 4679 ((2008)朝民初字第4679号).

781 *Universal Music v. Yahoo.cn (环球唱片诉雅虎侵犯信息网络传播权案)* (n771).

782 BaiduWenKu talks about copyright problem: we have notice-and-takedown procedure all the time ("百度文库谈版权问题：一直有通知删除机制"), 2010, http://tech.163.com/10/1125/12/6MB9I2TJ000915BF.html, Accessed September 17, 2014.

783 Guiding Opinions (指导意见) (n229), Art. 31.

784 "Hot-play" is a term that can always be found in the decisions made by Chinese courts, and finally was incorporated into the Provisions by Supreme Court. In terms of relevant decisions, "hot-play" has always been used to describe the audio-video works which are newly distributed, popular and still on screen.

785 Internet Provisions (n208) (draft) (网络规定征求意见稿), Art. 18.

786 Internet Provisions (n208) (draft) (网络规定征求意见稿), Art. 14.

In China, for some high valuable copyrighted contents, copyright owners tend to send notices to hosting ISPs even before these contents are officially released so as to alert the hosting ISPs about possible infringement. For such a kind of notice, some Chinese courts hold that it can impose a duty of care on hosting ISP to prevent relevant contents from being illegally uploaded. For instance, in the case of *China Film Group Corporation v. Ku6.com*, the plaintiff China Film Group Corporation owned the copyright of a movie "ChiBi", and before this movie was released, the plaintiff sent a notice, which warned of possible infringement, to the defendant who ran a platform for users to upload videos. However, the movie could still be accessed by the public on the defendant's platform afterwards, so the plaintiff sued the defendant for copyright infringement. The first Intermediate Court of Beijing held that after receiving warning notice, the defendant should know the movie concerned could not be made available to the public without the permission of the plaintiff, but this movie was still publicly accessible on its platform, which demonstrated that the defendant did not fulfill its duty of care and was therefore liable.[787]

5.4 Comparison between the US, the EU and China

Notice-and-takedown procedure was first adopted by *DMCA* 512, which aims at efficiently reducing copyright infringement on the Internet without involving time-consuming trials.[788] According to this procedure, an ISP needs to remove the alleged infringing materials upon receiving competent notices. In the US, a competent notice does not need to include the evidence of infringement but only a statement of alleging infringement, which means hosting ISPs do not need to assess whether the materials complained about in notices are infringing and it is therefore irrelevant whether notices can actually result into ISPs' knowledge of infringement.[789] The notice-and-takedown procedure in China shares many common features with the US one, but a notice should include evidence about infringement so as to be held competent. In this sense, hosting ISPs in China are supposed to assess the infringing evidence indicated in notices, and then decide whether to remove the materials that are complained about in the notices. In the EU, notice-and-takedown procedure has not been codified at the EU level, and normally the takedown obligation only can be provoked where notices can lead to ISPs' knowledge of infringement.[790] Therefore, a competent notice in the EU should include evidence about complained infringement, and thus hosting ISPs are supposed to assess

787 *China Film Group Corporation v. Ku6.com (中国电影集团诉酷6网侵犯信息网络传播权案)*, Beijing First Intermediate Court (北京市第一中级人民法院), YiZhongMinZhongZi No.5514 ((2009)一中民终字第5514号案).

788 H.R. REP. 105-551(II) (n16), at 54.

789 Holznagel, 'Melde- und Abhilfeverfahren zur Beanstandung rechtswidrig gehosteter Inhalte nach europäischem und deutschem Recht im Vergleich zu gesetzlich geregelten notice and take-down-Verfahren' (n63), at 106.

790 Ibid, at 107.

that evidence before removing the infringing materials alleged in notices.[791]
Generally, codified notice-and-takedown procedures can achieve a better legal certainty, since many issues involved in notice-and-takedown procedures have been clarified at the legislative level. These issues are: (1) hosting ISPs should designate a specific agency to receive notices; (2) the elements should be included in a competent notice; (3) hosting ISPs should forward the complaining notices to the Internet users whose content is removed; (4) the elements of counter-notice; (5) hosting ISPs should replace the removed content after receiving counter-notices; (6) who should be liable for wrong deletion. The clarification of these issues helps the concerned parties, including copyright owners, hosting ISPs and Internet users, know the rights and obligations they have, which can make the notice-and-takedown procedures run more smoothly. Particularly, the codified notice-and-takedown procedures authorize Internet users to send counter-notices, by which internet users can replace their legal content which has been wrongly taken down. Nevertheless, despite the many differences at legislative level, when ruling on notice-and-takedown procedures, the courts in the US, EU and China do encounter some common problems, which will be discussed in the following section.

5.4.1 The Locations of Infringing Materials

In the countries which set a requirement on notice at legislative level, the locations
176 of infringing materials need to be included in a competent notice, such as in the US, China, the UK, France and Finland discussed above. In Germany and Italy, the case law also requires the notice to at least include sufficient information for ISPs to locate the infringing materials.[792] How should a notice indicate the location of infringing materials? From the perspective of ISPs, the locations of infringing materials must be detailed enough for them to easily identify the alleged infringing materials, such as providing URLs.[793] However, rights holders argue that the specific information of infringing materials, such as URLs, should not be required as an essential element of a notice, since it would be burdensome for them.[794] The courts also have divergent opinions on this issue. A court in Italy held that the URLs should be offered in a notice so that the ISP can easily locate the infringing materials.[795] In the US, in the case of *Perfect 10, Inc. v. Google, Inc*, the court also held that the URLs had to be indicated in the notices as the information "reasonably sufficient to identify the location of infringing materials.[796] However, in Germany and China, the courts focus more on

791 As can be seen from the above discussion about notice-and-takedown procedures in the EU, the UK and France clearly provide that evidence about infringement should be included in notices. In Germany, according to case law, evidence of infringement also needs to be included in notices.
792 See Section 5.2.3. "Precise location of alleged infringing materials" above.
793 Commission Staff Working Paper: Online Services, Including E-commerce in the Single Market (n37), at 43.
794 Ibid.
795 Spedicato, 'Italy: the take-down notice must contain the specific YouTube URLs' (n437).
796 *Perfect 10, Inc. v. Google, Inc.*, No. CV 04-9484 AHM, 2010 WL 9479059 (C.D. Cal. July 26, 2010), at 14.

whether the information in notices is sufficient for ISPs to precisely locate the infringing materials.[797] In order to set a proper criterion on indicating the location of infringing materials, one should look into the purpose of sending notices. Sending notices aims at making the ISPs know precisely of which contents are infringing so that the ISPs can expeditiously remove these infringing contents. In this sense, providing URLs is the best way to fulfill this purpose. First, URLs (Universal Resource Locators) are Internet addresses which can "unambiguously resolve to a specific location where online resources can be found."[798] So alleged infringing materials can be precisely located, if the URLs are given in notices. Second, supplying the other location information, which is always search terms including names of authors, titles of works and albums, cannot ensure that all links generated from these search terms are to infringing materials.[799] In these circumstances, in order to avoid the wrong takedown, ISPs would be forced to investigate the entire websites on the basis of the search terms, which is too burdensome for them.[800] Further, the results generated via search terms are in "constant state of flux", and "there is no certainty that any particular search will yield the exact same results at different times."[801] So if recognizing search terms as competent location information, ISPs need to constantly monitor the results returned via the search terms. Finally, it is not unreasonably burdensome for copyright owners to supply the URLs of alleged infringing materials in notices, since copyright owners have agreed to do so according to the Code of Conduct reached with ISPs.[802] Therefore, it is reasonable to require the URLs of alleged infringing materials to be included in notices. By doing so, it not only can avoid imposing an unreasonable burden on hosting ISPs, but also can reduce the wrong deletion of Internet users' legal materials.

5.4.2 Expeditiously Remove

In order to avoid being held liable, upon receiving competent notices, ISPs should expeditiously remove the infringing materials alleged in the notices. How should "expeditiously remove" be defined? It is unrealistic to set a fixed term. The Chinese Supreme Court had tried to set a fixed term for removing, but finally failed.[803] In the

797 See Guiding Opinions (指导意见) (n229), Art. 28; see also BGH – *Stiftparfuem* (n718).

798 Seng D, 'The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices' (2014) 18 Virginia Journal of Law and Technology 369, at 396.

799 *Perfect 10, Inc. v. Giganews, Inc.*, 993 F. Supp. 2d 1192, at 1200-1201 (C.D. Cal. 2014).

800 Seng, 'The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices' (n793), at 398.

801 *Perfect 10, Inc. v. Giganews, Inc.*(n794), at 1200-1201.

802 See Notice-and-Takedown Code of Conduct, Art. 4b(2). The detailed discussion about this Code of Conduct will be done in Section 7.1.1. Code of Conduct means the self-regulation agreement reached between multiple copyright owners and hosting ISPs, and it aims at reinforcing the cooperation between them so as to reduce copyright infringement on the Internet. See Section 7.1.

803 As discussed above in the Chinese part, according to the Internet Provisions (draft), except having reasonable excuse, the ISPs should take necessary measures against infringing materials in a working day after receiving competent notice if the notice complains about illegal transmission of hot-play movies or TV series, but for the other types of work, ISPs should take necessary measures in no more than 5 working days. However, in the final version, this article was deleted.

EU, most member states do not define "expeditiously removing" in a fixed term at legislative level, and even most of notice-and-takedown agreements between right holders and ISPs do not specify a fixed term for takedown.[804] Therefore, this issue is mainly left for courts to decide case-by-case. The Chinese Supreme Court enumerates several factors for courts to decide whether takedown has been expeditiously done in the Internet Provision,[805] which can offer us some useful clues. For example, the way of sending notice should be considered, so if the URLs of infringing materials indicated in photocopies rather than in e-format, it will take more time to fulfill the takedown obligation.[806] Further, the following facts also result in a longer takedown-term, such as the notice is less accurate, the takedown measure is hard to conduct, and too many materials need to be removed.[807] However, if in a notice, a famous or popular work is alleged to be infringed, the ISP is expected to takedown infringing materials more quickly than usual.[808]

5.4.3 Substantially Comply or Fully Comply

Instead of requiring "substantially" comply with elements of notice like *DMCA* 512 in the US,[809] in China, the Internet Regulation reads "notice shall contain the following elements".[810] If following literal interpretation, the text in the Internet Regulations should be interpreted in such a way, namely, a competent notice should fully comply
178 with elements of notice, and only substantially complying is not enough.[811] However, according to the Beijing Higher Court, it seems to be sufficient for a notice to substantially comply with the elements. In the Guiding Opinions of the Beijing Higher Court, Article 28 reads that "if a notice sent to an ISP by the right owner does not include the web address of the alleged infringing material, but the information provided in the notice is sufficient for the ISP to accurately locate the alleged infringing material, the notice sent by the right owner can be determined to be" competent.[812] So if the information offered in a notice can substantially function like a web address, the notice can be held competent. In the EU, the ECJ holds a similar view. In the case of *L'Oréal SA v. eBay*, the ECJ held that when a notice is not sufficiently precise or properly substantiated, the information included in the notice still should be taken into account by the courts in Member States when determining whether a hosting ISP is aware of illegal activity

804 Commission Staff Working Paper: Online Services, Including E-commerce in the Single Market (n37), at 44.
805 Internet Provisions (网络规定) (n208), Art. 14.
806 Ibid.
807 Ibid.
808 Ibid.
809 According to DMCA (n1), Sec. 512 (c)(3)(B)(i), a notice only needs to substantially comply with elements of notice so as to be valid.
810 Internet Regulation (网络条例) (n1), Art. 14.
811 Wan Y, 'Safe Harbors from Copyright Infringement Liability in China' (2012) 60 Journal of the Copyright Society of the U.S.A 635, at 652.
812 Guiding Opinions (指导意见) (n229), Art. 28.

which is the subject of the complaint.[813] Therefore, once receiving an incompetent notice, the hosting ISP may still need to promptly remove the materials complained of in the notice, if hosting ISP can know the materials based on the information provided in the notice.

Further, a notice, which does not substantially comply with the requirement, may still arouse the hosting ISP's obligation to help the notifier perfect the notice. For instance, in the US, a hosting ISP is obligated to contact the notifier and help it make the notice substantially comply with the requirement, if the notice includes the following information: (1) identification of the copyrighted work claimed to be infringed, (2) identification of the material that is claimed to be infringing, (3) the information permits the infringing materials to be located, (4) the contact information that allows the notifier to be contacted.[814] Similarly, in Germany, in the light of the Federal Supreme Court, if a notice includes the clear indication of the specific infringing materials, but the hosting ISP has reasonable doubts about the legality of the notice, it is obligated to ask the notifier to provide relevant evidence to justify that indication.[815] These reasonable doubts include whether there exists a valid right, whether the notifier is authorized to enforce this property right and whether the reported facts about the infringement are true.[816] Therefore, when a notice includes sufficient information to have the materials identified and located, which can arouse hosting ISPs' strong suspicion that the materials complained about are infringing, the hosting ISPs are obligated to contact the notifiers and help them perfect the notices. In essence, the notice-and-takedown procedure works as a cooperative mechanism between copyright owners and hosting ISPs in respect of preventing infringement,[817] so it is reasonable to require hosting ISPs to fulfill a certain obligation to help copyright owners perfect their notices, when the notices can arouse hosting ISPs' strong suspicion that the materials complained of are infringing.

5.4.4 Wrong Deletion

In China, as mentioned above, copyright owners should be liable for the damages caused by the wrong deletion resulting from their mistaken notices.[818] Unlike DMCA 512, which only requires copyright owners to be liable for the wrong deletion if they "knowingly materially misrepresent" in the notices,[819] in terms of Internet Regulations,

813 *L'Oréal SA and Others v eBay International AG and Others* (n327), para. 122.
814 DMCA (n1), Sec. 512, c(3)(B)(ii).
815 BGH – Stiftparfuem (n718). The detailed discussion can be found in Section 5.2.4.
816 Ibid.
817 "safe harbor" provisions aim at encouraging the cooperation between copyright owners and hosting ISPs in protecting copyright, see H.R. REP. 105-551(II) (n16), at 50. The notice-and-takedown procedure is one of the mechanisms to fulfill this aim.
818 Internet Regulation (网络条例) (n1), Art. 24.
819 DMCA (n1), Sec. 512, (f).

copyright owners in China seem to undertake strict liability for wrong deletion.[820] In the EU Member States discussed above, Finland and France set an explicit provision on wrong deletion, according to which, right holders are only subject to liability if they send false notices in bad faith.[821] Theoretically, the Chinese approach encourages copyright owners to send notices with more diligence, which can effectively reduce wrong deletion; but the fault-based approach is friendlier for rights owners to curb large-scaled infringement by sending notices. Further, can an ISP be liable for wrong deletion? In China, if an ISP removes the suspicious materials by following the instruction in a notice, even though the suspicious materials are finally proved to be legal, the ISP need not be liable for wrong deletion,[822] as in the US[823]. In the EU, in some member states which have codified notice-and-takedown procedures at the legislative level, if ISPs conduct deletion by following the procedure in good faith, they are exempted from liability for any wrong deletion.[824] It is reasonable to grant liability exemption to these ISPs who faithfully follow the procedure. First, from the perspective of efficiency, if ISPs are subject to liability for wrong deletion conducted by following the notices, they tend to check each notice quite carefully, which will unavoidably reduce the efficiency of the procedure. Second, it's also too burdensome for ISPs to inspect each notice, since notices are always sent in large numbers.

180 ### 5.4.5 The Validity of Ex ante Notices

In order to protect better their interests, some copyright owners send notices to hosting ISPs even before the infringement actually occurs. In these cases, notices function more like warnings of possible infringement, and copyright owners expect that, upon receiving such warnings, hosting ISPs take necessary measures to prevent the materials indicated in the warnings from being uploaded without permission. Regarding ex ante notices, the US courts dismiss the validity of them, but some Chinese courts recognize their validity.[825] This thesis argues that the validity of ex ante notices should not be endorsed by courts. First, in terms of the necessary elements of a competent notice, the warning notice cannot be held as competent under notice-and-takedown procedure, since it is impossible for a warning notice to indicate the location of infringement or include any infringing evidence before the infringement actually occurs. Besides, if the validity of a warning notice is admitted, hosting ISPs need to actively check all of the materials

820 Article 24 of Internet Regulation reads that "if the relevant ISP, as a result of the copyright owner's notice, wrongly deletes or cuts off the link to any work, performance, recording or audio-visual product and therefore causes any damage to its service recipient, the copyright owner shall be subject to compensation." No fault requirement can be found in this Article.

821 LCEN (n171), Art. 6-I-4.

822 Article 24 of Communication Regulation makes it clear that copyright owners rather than ISPs should be liable for the wrong deletion caused by notices.

823 DMCA (n1), Sec. 512, (g)(2).

824 Commission Staff Working Paper: Online Services, Including E-commerce in the Single Market (n37), at 45.

825 See what have been discussed in Section 5.1.2 and Section 5.3.

uploaded by their users so as to filter out the possible illegal uploading referred in the notice. Therefore, admitting the validity of a warning notice seems to also conflict with a statutory doctrine in "safe harbor" provisions, and it is that no general monitoring obligation should be imposed on hosting ISPs.

5.5 Rethinking of Notice-and-takedown Procedures

In the Internet age, copyright owners lose their control on copyrighted works, and the piracy emerges on a large scale, so notice-and-takedown procedure, which can take down the infringing materials without judicial reviewing, has a big advantage of efficiently curbing piracy. However, lots of criticism has been aroused against notice-and-takedown procedure, since it may erode other rights while strengthening copyright protection.[826] Particularly, the notice-and-takedown procedure is easy to be misused, and for example, "in 2007, Viacom sent 100,000 takedown notices to YouTube, en masse, including takedown notices for materials to which it did not own the copyright."[827] In order to avoid being liable, a hosting ISP is prone to remove the material complained about in the notice without examining whether the material is actually infringing or not.[828] Therefore, legal materials are possibly being removed based on mistaken notices.

5.5.1 Wrong Deletion Resulting from Current Notice-and-takedown Procedures

In the US, the notice-and-takedown procedure favors copyright owners, upon receiving a competent notice, the hosting ISP should immediately remove the alleged infringing material, and no judicial review is needed.[829] As a competent notice, it's unnecessary to offer evidence about infringement, but merely include a statement made by copyright owners under penalty of perjury, which asserts the truth of the claim against copyright infringement.[830] However, it seems that a statement under penalty of perjury cannot always prevent copyright owners from sending false notices, and actually, DMCA takedown notices are commonly faulty.[831] After examining how a notice is sent, one may not be so surprised about why notices are commonly faulty. Since too many notices need to be sent, the copyright owners often "do not bother to check whether an item is truly infringing," but rely on automated programs to identify the infringing materials by using "titles of copyright works and fragments of copyrighted songs or videos" as searching

826 See Seltzer, 'Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment' (n36).

827 Cobia J, 'The Digital Millennium Copyright Act Takedown Notice Procedure: Misuses, Abuses, and Shortcomings of the Process' (2008), 10 Minnesota Journal of Law, Science & Technology 387, at 392.

828 Moore and Clayton, 'The Impact of Incentives on Notice and Take-down' (n63), at 244.

829 DMCA (n1), Sec. 512 (c)(1)(C).

830 DMCA (n1), Sec. 512 (C)(3)(v), (vi).

831 Murtagh MP, 'The FCC, the DMCA, and Why Takedown Notices are Not Enough' (2009) 61 Hastings Law Journal 233, at 254.

keywords.[832] If any matching material is found, a notice will be sent to the relevant ISP, and request the takedown of that material without any cautious examination.[833] This may explain why YouTube was ordered to take down a video entitled *Beijing Olympic Opening Ceremony* by International Olympic Committee, but the video turned out to be a record of a protest with just a few clips copyrighted by the International Olympic Committee.[834]

Why can copyright owners send notices without diligent investigation? This can be explained by two reasons: first, the public whose materials are wrongly removed rarely send counter notifications or file lawsuits against the copyright owners who send wrong notices;[835] second, copyright owners need to pay damages caused by mistaken notices only when they "knowingly materially misrepresent" in the notice.[836] In terms of the US courts, "knowingly materially misrepresent" is a high standard to reach. In the case of *Rossi v. MPAA*, the defendant MPAA sent a notice to a corresponding ISP and complained that the movies copyrighted by it were downloadable on the plaintiff's website, which resulted in the plaintiff's website being blocked by the ISP; however, the notice turned out to be mistaken, so the plaintiff sued the MPAA based on "misrepresentation" clause.[837] Finally, the 9th Cir. Court held that, the cause of paying damage under "misrepresentation" clause was limited to situations where the misrepresentation was "knowing", and that a subjective belief that materials were infringing, even if the belief was incorrect, did not qualify as a "knowing" misrepresentation.[838] Besides the MPAA in this case, other copyright owners have also been held as not liable for sending wrong notices,[839] and as noted by Urban and Quilter, no claims based on the "misrepresentation clause" succeeded except in the case of *Online Policy Group v. Diebold*,[840] where the defendant Diebold sent a notice complaining about a clear fair use of its materials.[841] In order to protest against the misuse of a takedown notice, a website called "Chilling Effects

182

832 Seidenberg S 'Copyright in the Age of YouTube' (2009) 95 ABAJ 46, at 48.

833 Ibid.

834 Ibid.

835 Cobia, 'The Digital Millennium Copyright Act Takedown Notice Procedure: Misuses, Abuses, and Shortcomings of the Process' (n822), at 391. See also Seng, 'The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices' (n793), at 48.

836 DMCA (n1), Sec. 512, (f).

837 *Rossi v. Motion Picture Ass'n of America*, 391 F.3d 1000, at 1001-1002 (9th Cir. 2004).

838 Ibid, at 1004-1005.

839 See *Dudnikov v. MGA Entertainment, Inc.*, 410 F. Supp. 2d 1010 (D. Colo. 2005); *Arista Records, Inc. v. Mp3Board, Inc.* (n678).

840 *Online Policy Group v. Diebold, Inc.* (n690). In this case, the defendant produced voting machines, but these machines were criticized as inaccurate. In early 2003, an archive of internal emails among the defendant's employees was revealed on the Internet, and some of these emails included evidence of the machines' inaccuracy. The plaintiffs Pavlosky and Smith wrote and published an article criticizing the defendant's machines and containing a hyperlink to the email archive. The court held that the plaintiff's use of the email archive is obviously a fair use, so the defendant knowingly misrepresented when sending the takedown notice.

841 Urban and Quilter, 'Efficient Process or Chilling Effects-Takedown Notices under Section 512 of the Digital Millennium Copyright Act' (n38), at 629-630.

Clearinghouse" has been set up to allow the public to report the notices they receive.[842] In the light of research done on the 876 notices reported to Chilling Effects, Urban and Quilter noted that nearly 30% of takedown notices sent to Google were based on flawed or highly questionable copyright claims.[843] Other research done by Brennan Center for Justice at New York University revealed that, among 245 takedown notices reported to Chilling effects in 2004, 63% of the notices "either targeted material with a fair use/First Amendment defense or stated a weak IP claim."[844]

Therefore, the current notice-and-takedown procedure will unavoidably lead to negative effects, such as suppression of fair use, freedom of speech and competition[845]. In order to test the possible suppression of fair use resulting from the notice-and-takedown procedure, Prof. Wendy Seltzer posted a clip of the NFL's (National Football League) copyright notice on YouTube.[846] Unsurprisingly, the NFL sent a takedown notice to YouTube, and then the video was removed.[847] Soon afterwards, Prof. Seltzer sent a counter notice, which claimed a fair use defense on the basis that the video clip was used for critical and educational purposes, and then the video was replaced by YouTube.[848] However, instead of suing Prof. Wendy for infringement, the NFL sent another takedown notice to YouTube, and the video was removed again.[849] It deserves attention that the NFL clearly knew of Prof. Seltzer's fair use claim on its video, since the counter notice must have been forwarded to the NFL.[850] So the NFL was supposed to launch a lawsuit against Prof. Wendy, but in the case that a takedown notice could easily remove the video without the need of overthrowing a fair use defense, the NFL decided to send another notice. Furthermore, the notice-and-takedown procedure has also been used to hinder criticism against copyright owners, which freezes the freedom of speech. In one instance, a blogger named Michelle Malkin made a video to criticize the rapper Akon, and then posted the video on YouTube.[851] In order to support her argument, several excerpts from Akon's music videos were incorporated into the video, and later on, the video was complained about by Akon and United Music Group based on copyright

842 See https://www.chillingeffects.org/index.cgi, (last visited 22-08-2014).

843 Urban and Quilter, 'Efficient Process or Chilling Effects-Takedown Notices under Section 512 of the Digital Millennium Copyright Act' (n38), at 667.

844 Heins and Beckles, *Will Fair Use Survive? Free Expression in the Age of Copyright Control,* at 35.

845 Regarding competition concern, it mainly focuses on the notice sent to search engines, such as Google. In the light of research done by Urban and Quilter in 2005, "a large percentage of Google search notices – 55% of the Google § 512(d) notices – are competition – related." See Urban and Quilter, 'Efficient Process or Chilling Effects-Takedown Notices under Section 512 of the Digital Millennium Copyright Act' (n38), at 651.

846 Lattman P, *Law Professor Wendy Seltzer Takes on the NFL*, Law Blog - WSJ.com(2007), *available at* http://blogs.wsj.com/law/2007/03/21/law-professor-wendy-seltzer-takes-on-the-nfl/ (last visit 25-08-2014).

847 Ibid.

848 Ibid.

849 Ibid.

850 DMCA (n1), Sec. 512, g(2)(B).

851 *Music Publisher Tries to Muzzle Podcast Criticizing Akon*, Electronic Frontier Foundation(2007), *available at* https://www.eff.org/takedowns/music-publisher-tries-muzzle-podcast-criticizing-akon, (last visited 25-08-2014).

infringement, so YouTube took the video down.[852] Fortunately, with help from the Electronic Frontier Foundation, Michelle Malkin sent a counter notice to YouTube, and successfully forced the UMG to rescind its takedown request.[853] In another instance, Randy Queen, as a comic book artist, found an article criticizing his way of depicting women was posted on the blog Escher Girls, and then he sent a takedown notice to the host Tumblr on the basis that some of his copyrighted comic illustrations were cited in the article, although these illustrations were definitely incorporated for supporting the author's argument.[854] As has been pointed out above, counter notices are really rare, so the copyright owners have a big chance to suppress the criticism against them.

Besides, notice-and-takedown procedure has also been used by companies for filtering out the information that might negatively affect their business. For instance, Yahoo sent a takedown notice to Cryptome, and complained about a report published on Cryptome which revealed that Yahoo was logging its users' data and selling these data to the law enforcement agencies.[855] Since the leak of Yahoo's bad privacy policy was likely to worsen its reputation and make it less competitive, Yahoo attempted to get rid of these leaks by abusing the notice-and-takedown procedure.[856] In another case, a voting machine company's internal documents, which discussed the flaws of its voting machine, were revealed on the Internet.[857] In order to suppress criticism of the flaws of its voting machine, the company filed dozens of notices to the ISPs who hosted the
184 leaked internal documents, and claimed these documents were copyrighted by it.[858] Although these documents were almost certainly covered by fair use, many hosting ISPs removed the document without checking the adequacy of the notice.[859]

In the EU, notice-and-takedown procedures have been developed based on the fact that notices can result in hosting ISPs' knowledge provided in Article 14 of the E-commerce Directive, so unlike the notice sent in terms of DMCA 512 c(3)(A), the notices under the EU regime should include the evidence to prove that the disputed materials are infringing.[860] Therefore, the notice-and-takedown procedure is supposed to be less

852 Ibid.

853 *Universal Music Group Backs Off Claims to Michelle Malkin Video*, Electronic Frontier Foundation(2007), *available at* https://www.eff.org/deeplinks/2007/05/universal-music-group-backs-claims-michelle-malkin-video (last visited 25-09-2014).

854 David Lizerbram, *Using Copyright to Suppress Criticism?*, David Lizerbram & Associates(2014), *available at* http://lizerbramlaw.com/2014/08/using-copyright-suppress-criticism/, (last visited 25-09-2014).

855 Kim Zetter, *Yahoo Issues Takedown Notice for Spying Price List*(2009), *available at* http://www.herbogeminis.com/IMG/pdf/yahoo.pdf, (last visited 26-08-2014).

856 Ibid.

857 Paul Roberts, *Diebold Voting Case Tests DMCA*, PCWorld(2003), *available at* http://www.pcworld.com/article/113273/article.html (last visited 27-11-2014).

858 Ibid.

859 Ibid.

860 Holznagel, 'Melde- und Abhilfeverfahren zur Beanstandung rechtswidrig gehosteter Inhalte nach europäischem und deutschem Recht im Vergleich zu gesetzlich geregelten notice and take-down-Verfahren' (n63), at 107. From the text discussing notice and takedown procedure in the EU, it can be concluded that evidence about infringement is required to be offered in a notice by either the courts or legislations in the member states.

vulnerable to abuse in the EU, since each notice needs to incorporate evidence that can prove alleged infringement. However, actually, the notice-and-takedown procedures are also vulnerable to be misused in the EU, since the EU regime creates incentives for ISPs to remove the disputed materials after receiving notices.[861] In an experiment done by an Oxford research group, the UK hosting ISP is even more prone to follow a false notice, since no statement under penalty of perjury is required by UK law.[862] Similarly, an experiment done in the Netherlands also demonstrated that the ISPs are generally keen to avoid the liability without considering the accuracy of notices.[863] In this experiment, some materials which were not protected by copyright anymore were posted onto the Internet, and then the researcher sent notices to 10 relevant Dutch ISPs; finally, seven of ten ISPs had removed the materials, and no one ever complained about these mistaken deletions.[864] In the Member States which haven't ruled on the minimum elements of a notice, the hosting ISPs prefer to remove more suspicious materials rather than keep them online, since the hosting ISPs only have a tiny interest in each of these suspicious materials but face the threat of paying high cost for keeping them.[865] As noted by Christian Ahlert, in the EU, the current regulatory mechanism regarding notice-and-takedown procedure "has created an environment in which the incentive to take down content from the internet is higher than the potential costs of not taking it down."[866]

5.5.2 How to Reduce Wrong Deletion

Therefore, some measures should be taken to reduce wrong deletion. During the public consultation on the EU Notice and Action procedures, civil society organizations expressed their concerns on the possible wrong deletion under these procedures, and made some proposals to reduce wrong deletion.[867] Regarding how to reduce the wrong deletion, it is necessary to check the reasons that result in the wrong deletion. Based on the above discussion, it can be found that wrong deletion can be attributed to three reasons. First, copyright owners tend to send notices without diligent investigation. Second, hosting ISPs are highly likely to remove the materials complained of in the notices so as to reduce the risks of being sued by copyright owners. Third, Internet users normally do not send counter-notices even when their materials are wrongly taken down.

861 Moore and Clayton, 'The Impact of Incentives on Notice and Take-down' (n63), at 243

862 Ibid, at 243-44.

863 Ibid, at 244.

864 Ibid, at 244.

865 See Holznagel, 'Melde- und Abhilfeverfahren zur Beanstandung rechtswidrig gehosteter Inhalte nach europäischem und deutschem Recht im Vergleich zu gesetzlich geregelten notice and take-down-Verfahren' (n63), at 106.

866 Ahlert C, et al., How 'liberty' disappeared from cyberspace: the mystery shopper tests Internet content self-regulation (2004), RootSecure.com, available at http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf (last visited 08-12-2014), at 11. In this article, the author explains why the ISPs tend to take down the suspicious materials after receiving notices.

867 Kuczerawy, A., Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative (2015) 31 Computer Law & Security Review 46, at 52-55.

Therefore, all three stakeholders, including copyright owners, hosting ISPs and Internet users, contribute to the wrong deletion. But who should be given the burden of reducing the number of wrong deletions? To answer this question, we need to examine how the notice-and-takedown procedure operates. Basically, the notice-and-takedown procedure can be simply described as "copyright owners notice and hosting ISPs take down", so it has been implied that copyright owners bear the burden of seeking infringing materials, and hosting ISPs are just the facilitators who help copyright owners enforce their rights. Therefore, this thesis argues that copyright owners should ensure the accuracy of their notices so as to reduce the wrong deletions. This argument also echoes the recent case law in the US. In order to curb notice-and-takedown procedure's possible suppression on free speech, the US courts have started to require copyright owners to take fair use into account. For example, in the case of *Lenz v. Universal Music Corp.*, the defendant Universal Music Corp. was held liable under a mis-representation clause, because it failed to consider whether the plaintiff's incorporation of its music into a homemade video was fair use, before sending a takedown notice to YouTube.[868] Further, it is also unreasonable to require hosting ISPs to ensure the takedown is correctly made, since it would force the hosting ISPs to evaluate the notices like judges which they are not able to do. As mentioned above, in France, some effort has been made to reduce the wrong deletions by imposing duties on hosting ISPs. French Constitutional Council held, only
186 when materials are manifestly unlawful or the court issues an order to remove, need hosting ISPs expeditiously remove the materials in question.[869] By doing so, the wrong removing is supposed to be reduced, since hosting ISPs are not obligated to take down the materials which are not manifestly unlawful. Nevertheless, regarding what constitutes "manifestly unlawful" materials, French Constitutional Council did not specify more on this notion.[870] If a clear definition has not been given to "manifestly unlawful" by courts, hosting ISPs tend to remove the suspicious materials so as to secure their immunity. In fact, unlike child pornography which is identifiable for any non-lawyer, in the context of copyright, whether a material is manifestly infringing is much more problematic to decide, and often can only be answered with professional legal advices.[871] Considering that notices might be received on a large scale every day, it seems still too burdensome for ISPs to seek professional legal advice for each notice. Regarding Internet users, although they are authorized to send counter-notices to have the removed materials replaced, they normally lack the expertise to decide whether the materials removed are legal or illegal. Particularly, after receiving the copies of the notices which alert them to the copyright infringement they might commit, they will be deterred from sending counter-notices.

868 *Lenz v. Universal Music Corp.*, 572 F. Supp. 2d 1150 (N.D. Cal. 2008).

869 Catherine Jasserand, *France- Dailymotion heavily fined for the late removal of infringing content*, wolters kluwer law & business (2012), *available at* http://kluwercopyrightblog.com/2012/09/28/france-dailymotion-heavily-fined-for-the-late-removal-of-infringing-content/, Accessed September 28, 2014.

870 Ibid.

871 Verbiest T et al., Study on the Liability of Internet Intermediaries (n389), at 41.

5.6 Conclusion:

In the US and China, notice-and-takedown procedure is a codified procedure, so once a hosting ISP receives a notice including the essential elements prescribed by the laws, the hosting ISP is obligated to take down the materials indicated in the notice. Nevertheless, unlike the US, in China a competent notice should include the evidences of complained infringement, so hosting ISPs are supposed to assess these evidences to decide whether the complained materials are actually infringing before taking down them. In the EU, the regulations on notice-and-takedown procedure turn out to be fragmented, but generally, in the Member States when a notice can lead to a hosting ISP's knowledge of infringing materials, the hosting ISP is obligated to take down the materials. In general, the codified notice-and-takedown procedures are preferable to de facto notice-and-takedown procedures developed in judicial practice, since the codified ones can provide better legal certainty to hosting ISPs. Nevertheless, no matter whether the notice-and-takedown procedure has been codified, the courts in these jurisdictional areas face the similar problems when ruling on notice-and-takedown procedures. These problems are as follows: how to define a competent notice, how to deal with the defect notices, how to define "expeditiously remove", how to distribute the liability for wrong deletion, and the validity of ex ante notices. The answers to these problems have substantial impacts on the hosting ISPs' freedom to operate. Regarding how to define a competent notice, the dispute mainly focuses on how exactly the location of alleged infringing materials should be indicated in notices. This book argues that it is reasonable to require copyright owners to provide the URLs of infringing materials, and by doing so, hosting ISPs face less burden to locate the infringing materials. Regarding how to deal with defect notices, if a notice is not fully but substantially comply with the requirement, its validity ought to be endorsed. If a notice is neither fully nor substantially comply with the requirement, but arouses the hosting ISP's strong suspicion of the existence of specific infringing materials, in the case of the contact of the notifier having been given, the hosting ISP is obligated to contact the notifier so as to help the notifier perfect the notice. Regarding "expeditiously remove", it is unpractical to set a fixed term, and courts should decide in light of concrete facts in each case. As for who should be liable for wrong deletion, hosting ISPs are immunized for liability if they conduct the deletion by following notices. Further, copyright owners are required to send notices in good faith, and otherwise, they should be liable for wrong deletion. Regarding ex ante notices, their validity ought to be dismissed, since if admitting the validity of ex ante notices, hosting ISPs would be imposed a general monitoring obligation which is forbidden by "safe harbor" provisions.

Although the current notice-and-takedown procedures contribute a lot to take down large-scale infringement on Internet, they also tend to result in wrong deletion. On one side, because internet users usually will not argue even if their legal contents were

removed, copyright owners are encouraged to send notices without seriously taking accuracy into account. On the other side, hosting ISPs tend to follow the notices no matter whether the notices are correct or wrong, since by doing so, they at least can avoid being sued by copyright owners. In order to substantially curb the wrong deletion under notice-and-takedown procedures, copyright owners rather than hosting ISPs should be imposed more duties to ensure the accuracy of notices, such as taking fair use into account when sending notices.

To sum up, copyright owners should play an active role in notice-and-takedown procedure. They shoulder the duty to seek infringing materials, notify hosting ISPs, and ensure the accuracy of notices. To the contrary, hosting ISPs are passive actors in this procedure, and their responsibilities are to properly respond to notices, such as conducting takedown after receiving competent notices, forwarding notices and counter notices, and informing copyright owners after receiving incompetent notices. This book asserts, by following this approach of distributing duties between copyright owners and hosting ISPs, it can avoid imposing an unreasonable burden on hosting ISPs in notice-and-takedown procedures, and is thus capable of preserving maximum freedom for hosting ISPs to operate in the US, EU and China.

Chapter 6

Disclosure of Internet Users' Identities in the US, EU and China

Introduction:

The Internet users, who commit infringement directly, as primary infringers, should be liable for the infringement. However, Internet is characterized with anonymization, which means that Internet users can easily hide their identities on the Internet. Without knowing the identities of infringers in suspect, copyright owners cannot launch lawsuits. In order to ensure the copyright owners' right to sue Internet users, the laws require ISPs to disclose the Internet users' identities under certain circumstances. At international level, Trips-plus provisions such as ACTA also include a clause which requires ISPs to disclose the identity information of suspected infringers to intellectual property owners.[872] However, Internet users' identities fall within the privacy which should be protected as one of the fundamental rights. Therefore, certain degree of restriction has to be rendered on identity disclosure in the context of copyright enforcement. From the perspective of avoiding conflicts with copyright owners, hosting ISPs are more willing to disclose the identity information requested by them, but such disclosure ought to follow due process because of privacy concerns. This chapter explores the identity disclosure mechanisms in the US, EU and China, and then discusses how to regulate hosting ISPs' duties in identity disclosure mechanisms from the perspective of preserving their freedom to operate.

This chapter first examines the rules on identity disclosure in the US, including the identity disclosure provided in "safe harbor" provisions and the "John Doe" subpoena developed from case law (6.1). Then, it looks into how the EU deals with identity disclosure in the context of copyright enforcement (6.2). In China, hosting ISPs need to disclose personal identity to Copyright Administrations and copyright owners upon request, and this chapter particularly examines the disclosure of personal identity in civil proceeding in China (6.3). Based on the exploration in the last three sections, it compares the hosting ISPs' duties in identity disclosure mechanisms in the US, EU and China, and then discusses how to regulate hosting ISPs' duties in solving the problems of current identity disclosure mechanisms (6.4).

6.1 Disclosure of Identities in the US

DMCA 512 (h) grants copyright owners the rights to apply subpoenas for the purpose of disclosing Internet users' identities. In the light of this Article, in the prescribed circumstances, a copyright owner or its agents can request the clerk of any US District Court to issue a subpoena for disclosing the identity of an alleged infringer.[873] A competent request for subpoena should include a copy of a notification according to DMCA 512 (c)(3)(A), a proposed subpoena, and a sworn declaration to indicate that the purpose of obtaining the identity of an alleged infringer is only for "protecting

872 Anti-Counterfeiting Trade Agreement, Art. 4.

873 DMCA (n1), Sec. 512 (h)(1).

rights under this title."[874] A proposed subpoena shall authorize and order the ISP concerned, based on the identity information it has about the alleged infringer in the notification, to expeditiously disclose sufficient information for the copyright owner or his authorized agent to identify the alleged infringer.[875] If a request of subpoena fulfills the requirements above, the clerk will expeditiously grant the proposed subpoena.[876] Upon receiving the subpoena, the ISP should follow the order in the subpoena.[877]

What kind of ISPs falls into the coverage of subpoena? With the flourishing of p2p networks, this question aroused disputes between ISPs and copyright owners. In the case of *RIAA v. Verizon*, RIAA requested a subpoena to ask Verizon, an access provider, to disclose its Internet users who traded copyrighted music through p2p software.[878] In the first instance and appeal, RIAA's request was supported, but in the last instance its request was denied.[879] In the light of the final judgment, since DMCA 512 (h)(2) makes it clear that a competent request for subpoena should include "a copy of a notification described in subsection (c)(3)(A)", but the notification offered by RIAA did not satisfy subsection (c)(3)(A)(iii), a subpoena could not be issued to Verizon based on RIAA's request.[880] After losing in this case, the RIAA tried to seek similar subpoenas from ISPs in the 8th and 4th Circuits, but still failed, because these courts upheld the same reasoning which favored Verizon.[881] Therefore, in the U.S., the subpoena under DMCA 512 (h) can only be issued to ISPs who run caching, hosting or information location tool, but access providers are immune from such subpoenas.[882] YouTube, as a popular video-sharing platform, has received several subpoenas for disclosing its subscribers' identities. For example, in 2007, Twentieth Century Fox filed a subpoena for YouTube to get the identity of someone who uploaded several episodes of its popular television shows without permission.[883] In March 2007, Magnolia Studios also sought a subpoena

874 Ibid, (h)(2).

875 Ibid, (h)(3).

876 Ibid, (h)(4).

877 Ibid, (h)(5).

878 *RIAA v. Verizon Internet Services*, 240 F. Supp. 2d 24, at 24-26 (D.D.C. 2003).

879 See *RIAA v. Verizon Internet Services*, 240 F. Supp. 2d 24 (D.D.C. 2003), 257 F. Supp. 2d 244 (D.D.C. 2003), 351 F.3d 1229 (D.C. Cir 2003).

880 *RIAA v. Verizon Internet Services,* 351 F.3d 1229 (D.C. Cir 2003), at 1236. According to DMCA (n1), Sec. 512 (c)(3)(A)(iii), a notification must identify "the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material." Nevertheless, Verizon, as an Internet access provider, was not involved in storing the infringing materials, so it was impossible for Verizon to remove or disable the access to the infringing materials, and thus notifications send by RIAA could not be competent under Sec. 512 (c)(3)(A)(iii).

881 Shanahan CE, 'ACTA Fool or: How Rights Holders Learned to Stop Worrying and Love 512's Subpoena Provisions' (2011), 15 Marquette Intellectual Property Law Review 465, at 472.

882 Peguera, 'The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems' (n175), at 492.

883 *Cuban's film studio subpoenas Google over videos*, Reuters(2007), *available at* http://www.reuters.com/article/2007/03/07/google-cuban-idUSN0726738220070307. quoting Eugene C Kim, *YouTube: Testing the safe harbors of digital copyright law*, 17 S. Cal. Interdisc. LJ (2007). 142

for YouTube so as to identify the users who uploaded the videos copyrighted by it.[884] Besides, copyright owners can also file John Doe subpoenas to find out the identities of Internet users suspected of infringement.[885] The procedure for seeking John Doe Subpoenas basically works as follows: a copyright owner should first obtain the IP address of the alleged infringer and the alleged infringing materials available at that IP address, and then file a John Doe Subpoena to require the ISP to reveal the name and address associated with this IP address.[886] Compared to subpoena under DMCA 512 (h), filing a John Doe subpoena is more costly.[887] In determining whether to grant a subpoena, a court always needs to comprehensively consider the following factors: 1) the claim of copyright infringement involved, 2) the possibility that the identity information may be destroyed by the ISP, 3) the disclosure request is narrowly tailored, 4) the subpoena will substantially contribute to forwarding the case; 5) without the information requested by subpoena, the defendant cannot be identified.[888] Further, in order to protect Internet users' privacy and the other rights protected by the first amendment, ISPs are required to contact the Internet users before disclosing their identities so that the Internet users can file a motion to squash or modify the subpoenas.[889]

In order to disclose the Internet users' identities, it is somehow necessary for an ISP to retain Internet users' online data. Currently, in the US, there is no mandatory data retention law.[890] There were several bills which intended to require ISPs to retain online data, but eventually all of them failed to become law.[891] However, it seems that it's also not forbidden for an ISP to retain the Internet users' data, because obviously, the ISPs such as YouTube have long been retaining its subscribers' online data.[892] In 2008, Judge Louis Stanton granted the motion which required YouTube to turn over the usernames of users, what videos have been watched, and the users' computer addresses to Viacom and the other plaintiffs.[893]

6.2 Disclosure of Identities in the EU

In the EU, the European Parliament enacted several Directives to protect personal data, including Directive 95/46/EC (General Data Protection Directive) and Directive

884 Ibid.

885 Nathaniel Gleicher, *John Doe Subpoenas: Toward a Consistent Legal Standard*, The Yale Law Journal (2008).

886 Shanahan, 'ACTA Fool or: How Rights Holders Learned to Stop Worrying and Love 512's Subpoena Provisions', at 472.

887 Ibid.

888 *Artista Records, LLC v. Does 1-12*, 2008 U.S. Dist. LEXIS 82548, at 5.

889 Ibid, at 5-6.

890 *United States*, Electronic Frontier Foundation, *available at* https://www.eff.org/issues/mandatory-data-retention/us (last visited 20-08-2014).

891 Ibid.

892 Miguel Helft, *Google told to turn over user data of YouTube*, The New York Times(2008), *available at* http://agriculturedefensecoalition.org/sites/default/files/file/constitution_1/1G_2008_Viacom_Lawsuit_Google_YouTube_July_4_2008_NYTimes.pdf, (last visited 20-08-2014).

893 Ibid.

2002/58/EC (e-Privacy Directive). In light of Directive 95/46/EC, personal data is generally protected from being disclosed, but Article 13 opens a window for restriction on personal data protection, including where such restriction constitutes a necessary measure to safeguard "the protection of the data subject or of the rights and freedom of others."[894] Article 15 of the e-Privacy Directive also allows imposing certain restrictions on personal data protection, and according to the opinion delivered by the ECJ in the *Promusicae* case, Article 15 of the e-Privacy Directive should be read in conjunction with Article 13 of Directive 95/46/EC, so it is allowed by Article 15 of the e-Privacy Directive to restrict the protection of personal data when such restriction "is necessary to safeguard the rights and freedoms of others, including the right to property in civil proceeding."[895] Therefore, in the light of the Directives relevant to privacy protection, the protection of personal data can be restricted in IP infringement cases.

Besides these two Directives about data protection, some Directives on IP protection also include rules about disclosing personal data. According to Article 15(2) of the E-commerce Directive, member states may establish obligations for ISPs promptly to "inform the competent public authorities of alleged illegal activities undertaken or information provided by the recipients of their service or obligation to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements."[896] Further, Article 8 of IP Enforcement Directive requires member states to ensure that in a proceeding about IP infringement, courts may issue an order to disclose the identities of persons who conduct infringement on a commercial scale, upon receiving justified and proportionate request from the claimants.[897]

From the EU Directives referred above, it seems that identity information of persons is allowed to be disclosed if these persons are involved in IP infringement. However, the EU Directives are prone to be less explicit , so with regard to in what circumstances Internet users' identity information can be disclosed, it is necessary to explore the ECJ cases, the implementing regulations and case law in member states. The following sections will explore how several key issues in identity disclosure mechanism are dealt in the EU, including: (1) can identity disclosure be done in civil proceeding; (2) whether hosting ISPs are obligated to retain their users' personal data; (3) who can order hosting ISPs to commit identity disclosure.

894 Directive 95/46/EC (n1), Art. 13 (g).

895 Kuner C, 'Data protection and rights protection on the internet: The Promusicae judgment of the European court of justice' (2008) 30 European Intellectual Property Review 199, at 199.

896 E-commerce Directive (n1), Art. 15(2).

897 Directive 2004/48/EC (n83), Art. 8.

6.2.1 Identity Disclosure – Civil Proceeding or Only Criminal Proceeding

In the light of Article 13 of General data protection Directive and Article 15 of E-privacy Directive, restriction can be rendered on personal data protection for limited purposes, but most of these purposes clearly direct to preventing serious crime rather than protecting private interests.[898] Further, Directives relevant to IP enforcement also do not declare that personal data can be disclosed in civil proceedings.[899] Therefore, it becomes a question of whether member states are required or prohibited to disclose the personal data retained by ISPs in civil proceedings. According to the ECJ's viewpoint, "European legal framework is neutral in this regard."[900] In the case of *Promusicae v. Telefónica*, the ECJ held that it is not an obligation for member states to require ISPs to communicate personal data so as to guarantee the protection of copyright in the context of civil proceedings.[901] In another case named Tele2, the ECJ held that the relevant EU Directives did not prohibit member states from requiring ISPs to disclose personal traffic data for the purpose of enabling civil proceedings dealing with copyright infringements.[902] Further, in both these cases, the ECJ emphasized that when transposing the Directives relevant to communicate personal data, the member states should strike a fair balance between the various fundamental rights protected by European legal orders; and further, the authorities and courts in member states should take into account the fundamental rights and the general principles of community law, such as proportionality,
196 when applying and interpreting their national law about disclosing personal data.[903] So basically, the member states have a certain degree of freedom to establish their national rules about disclosing personal data in civil proceedings.

898 According to Article 13 of General Data Protection Directive, a restriction can be rendered on personal data protection when such a restriction constitutes a necessary measure to safeguard: (a) national security; (b) defence; (c) public security; (c) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected , even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others. In light of Article 15 of E-privacy Directive, the restriction on personal data protection must constitute a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system.

899 Article 15(2) of E-commerce Directive only indicates that an ISP can pass on Internet users' personal data to competent authorities upon request. Article 8 of IP Enforcement Directive only prescribes that in a proceeding about IP infringement, courts may issue an order to disclose the identities of persons who conduct infringement on a commercial scale, but does not clarify whether such disclosure can be made in civil procedure.

900 Kuner C, et al., Study on online copyright enforcement and data protection in selected Member States (2009), DG Internal Market and Service of European Commission, at 9.

901 Case C-275/06 *Productores de Música de España v Telefónica de España Sau ('Promusicae')* [2008] ECR I-00271, para. 71.

902 Case C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH* [2009] ECR I-01227, para. 47.

903 See *Productores de Música de España(Promusicae) v. Telefónica de España SAU* (n896), *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH* (n897).

In the member states, some of them have already established the rules on disclosing personal data for the purpose of enabling copyright litigations in civil proceedings. In Italy, according to the Article 156bis of Italian Copyright Law, "if the rights holder has seriously proved its claims and has indicated documents, elements and information in possession of the other party which confirms such claims, the court – upon the rights holder's request – can order the alleged infringer to show the documents or to supply the relevant information concerning third parties involved in the production and distribution of the infringing products."[904] In the UK, copyright owners can apply the "Norwich Pharmacal orders" from courts so as to request hosting ISPs to disclose their users' personal data retained by them.[905] In order to successfully bring a "Norwich Pharmacal orders" claim, the following conditions should be fulfilled: "(1) a wrong must have been carried out or allegedly carried out by a wrongdoer; (2) there must be the need for the order to enable action to be brought against the wrongdoer; and (3) the person against whom the order was sought must be somehow involved in the wrongdoing so as to have facilitated it, and must be able or likely to be able to provide the information necessary to enable the wrongdoer to be sued."[906] In Germany, in line with Section 101(1) of the Copyright Act, a copyright owner can request the court to issue an order that requires the ISP to disclose the identity of the user who commits copyright infringement on a "commercial scale."[907] As for what constitutes a "commercial scale," the court should evaluate on the basis either of the number of infringements or the severity of the infringement.[908] Therefore, Germany limits the disclosure of personal data within serious copyright infringement cases in civil proceedings.

6.2.2 The Retention of Personal data

In order to disclose the suspected infringers' identities, the personal data of the suspected infringer should be retained at the first place. In 2006, the EU enacted the Data Retention Directive, in the light of which member states should require ISPs to retain the data which are necessary to identify the subscribers or users for the purpose of the investigation, detection and prosecution of serious crime and the retention period is not less than six months but no more than two years from the date of the

904 Tasillo A and Sterpi M 'Italy' in Calame TJ and Sterpi M eds., *Copyright Litigation: Jurisdictional Comparisons* (European Lawyer 2015), at 216.

905 See Kuner C, et al., Study on online copyright enforcement and data protection in selected Member States (n895), at 24.

906 *Mitsui Limited v Nexen Petroleum UK Limited* [2005] EWHC 625 (Ch), quoting Kuner C, et al., Study on online copyright enforcement and data protection in selected Member States (n895), at 25.

907 Gesetz über Urheberrecht und verwandte Schutzrechte, Sec. 101 (1). As provided in this Article, any person who infringes copyright or another right protected under this Act on a commercial scale may be required by the injured party to provide information without delay as to the origin and the distribution networks of infringing copies or other products.

908 Ibid.

communication.[909] Can these data retained for combating serious crime be disclosed for the purpose of copyright enforcement? The ECJ agreed to such a disclosure in 2012. In the case of Bonnier Audio AB v Perfect Communication Sweden AB, the ECJ held that the Data Retention Directive should not be interpreted to prohibit an ISP in Civil proceedings from being ordered to give a copyright owner the information of the subscriber who was alleged to commit copyright infringement.[910]

Regarding whether hosting ISPs are obliged to retain personal data in the light of Data Retention Directive, the answer is probably not. According to Article 5 of the Data Retention Directive, the categories of data are "only to be retained with respect to fixed network telephony, mobile telephony, Internet access, Internet e-mail, and Internet telephony."[911] Since the online communication through hosting ISPs' services normally can be categorized as neither Internet e-mail nor Internet telephony, the hosting ISPs, including video platforms, Usenet, blogs, message boards, social networking platforms, etc., are not obliged to retain personal data generated in online communication processes.[912] Nevertheless, the member state, such as France, still enacted a legal decree to require hosting ISPs to retain significant amounts of traffic data and so-called identification data, which went beyond the requirement of the EU Data Retention Directive.[913]

In fact, the proportionality of the Data Retention Directive has been widely challenged.[914] In 2014, the ECJ ruled on the validity of the Data Retention Directive, and concluded that
198 the provisions in the Directive were not proportionate based on the following reasons: the retention of data was not precisely circumscribed to ensure that the retention was limited to what was strictly necessary; the Directive also did not provide for sufficient safeguards to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data, so it conflicted with Article 8[915] of the Charter of Fundamental Rights of the European Union.[916] Therefore, the data retention rules in the

909 Council Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105/54, Art. 1 and Art. 6.

910 Case C-461/10, *Bonnier Audio AB v Perfect Communication Sweden AB* [2012] ECLI:EU:C:2012:2190.

911 See Directive 2006/24/EC (n904), Art. 5. See also Feiler L, '*The legality of the data retention directive in the light of the fundamental rights to privacy and data protection*' (2010) 1 European Journal of Law and Technology 3, Para. 7.3.4.

912 Ibid.

913 Maxwell W, 'Systematic government access to private-sector data in France' (2014) 4 International Data Privacy Law 4, at 7.

914 Blakeney S, 'The Data Retention Directive: combating terrorism or invading privacy?' (2007) 13 Computer and Telecommunications Law Review 153, at 153. In Germany, the Constitutional Court even held that the two new Articles, which aimed at transposing the provisions in the Data Retention Directive, were are null and void, since they conflict with the right to privacy of telecommunications protected in Article 10 of the German Constitution. See Kaiser AB, 'German data retention provisions unconstitutional in their present form; decision of 2 March 2010, NJW 2010, p.833' (2011) 6 European Constitutional Law Review 503, at 509.

915 In the light of this Article, personal data "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."

916 Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications and others* [2014] ECLI:EU:C:2014:238.

EU need to be crafted and pay more attention to privacy protection. In these circumstances, whether France still requires hosting ISPs to retain Internet users' personal data remains uncertain before the relevant rules have been eventually revised.

6.2.3 Ordering the Disclosure of Personal Identity

Regarding who can order the hosting ISPs to disclose the suspected infringers' identities, in order to prevent personal identity from being inappropriately disclosed, normally any request of disclosing personal identity should be subject to judicial or administrative review in the EU.[917]

In France, ISPs are not allowed to disclose Internet users' personal identities to copyright owners' representatives, and they can only respond to the identity requests issued by a court or the administrative authority – Hadopi.[918] In light of Article L.331-21 of the French Intellectual Property Code, the Hadopi Commission "may obtain, for the purpose of investigation, any documents, regardless of the support used, including data stored and processed by ISPs."[919] The ISP can be requested to disclose the identity, postal address, electronic address and telephone number of a suspected infringer, if these data are necessary to establish the evidence of a copyright infringement.[920] If copyright owners want to obtain the identities of suspected infringers, they need to file lawsuits, and then the personal identities become judicial data which can be communicated to copyright owners by ISPs once the courts order such disclosure.[921]

In Germany, ISPs are also not allowed to disclose the personal identity to copyright owners based on the IP addresses submitted by copyright owners, since by doing so, ISPs would violate the obligation of keeping telecommunication secrecy.[922] Therefore, if copyright owners want to have the suspected infringers' identities disclosed, they need to bring claims to courts according to Section 101 (1) of the Germany Copyright Act.[923] For the purpose of investigating criminal activities, the criminal enforcement authorities in Germany may request ISPs to disclose the suspects' identities, but the order of disclosure still has to be issued by courts.[924] In exceptional circumstances, the order may also be issued by the public prosecution office, but this order will become ineffective if it is not confirmed by the judge within 3 days.[925] Therefore, in Germany, the disclosure order normally can only be issued by courts, no matter whether such disclosure is requested by copyright owners or criminal enforcement authorities.

917 Kuner C, et al., Study on online copyright enforcement and data protection in selected Member States (n895), at 4.
918 Ibid, at 28.
919 Ibid.
920 Ibid.
921 Ibid, at 29.
922 Ibid, at 35.
923 Gesetz über Urheberrecht und verwandte Schutzrechte (n902), Sec. 101 (1).
924 Criminal Procedure Code (Strafprozeßordnung, StPO), Sec. 100b (1).
925 Ibid.

In the UK, the personal data can be disclosed to the competent authorities, such as the police, the Serious Organized Crime Agency, HM Revenue and Customs, the Security Service, the Secret Intelligence Service and the Government Communication Headquarters.[926] If a copyright owner wants to know the identity of a suspected infringer, he has to bring a civil action that requests the court to issue a "Norwich Pharmacal order."[927]

6.2.4 Summary in the EU

In the EU, the relevant directives generally allow the Internet users' personal data to be disclosed for the purpose of fighting copyright infringement. But since the disclosure of Internet users' personal data might invade the Internet users' privacy, according to the ECJ decisions, the authorities and courts of the member states should ensure that such disclosure is not conducted in a way that conflicts with "those fundamental rights or with other general principles of Community law, such as the principle of proportionality."[928] Therefore, the member states can establish their own rules of disclosing personal data under the general principle set by the ECJ. In Member States, for the purpose of protecting privacy, the disclosure of personal identity can only be done according to the orders issued by courts or competent authorities. Besides, normally hosting ISPs are not subject to the obligation of retaining their users' personal data in the context of Data Retention Directive. After the Data Retention Directive was held disproportionate, the disclosure of personal identity may become even harder, since without data retention, no data can be disclosed.

6.3 Disclosure of Identities in China

In China, there are several rules about the disclosure of infringers' identities. According to the Article 13 of Internet Regulations, the administrative department of copyrights may, within the purpose of investigating into the infringements upon the right to network dissemination of information, require the relevant ISPs to provide such materials as the names, contact information, and the web addresses of its service recipients who are suspected of committing copyright infringement.[929] Further, where any Internet service provider refuses or delays to provide such identity information as the name, contact information and web address of its service recipients who are suspected of committing infringement, the administrative department of copyright shall give it a warning.[930] In the event of serious circumstances, the equipment such as computers that are mainly applied to provide the Internet service shall be confiscated.[931] From the provisions above,

926 Kuner C, et al., Study on online copyright enforcement and data protection in selected Member States (n895), 22.
927 Ibid, at 24.
928 *Productores de Música de España(Promusicae) v. Telefónica de España SAU* (n896), para. 68 and 70.
929 Internet Regulation (网络规定) (n1), Art. 13.
930 Ibid, Art. 25.
931 Ibid.

it seems that only the administrative department of copyright can request the Internet users' identity information from ISPs. Nevertheless, relevant Judicial Interpretations issued by People's Supreme Court grant copyright owners the right to request Internet users' identity information in civil procedures. In terms of Internet Interpretation (2006), copyright owners can request the registration information of Internet users from hosting ISPs for the purpose of suing the Internet users for copyright infringement, and if the hosting ISPs refuse to provide the registration information at request without fair reasons, they need to undertake the liability accordingly.[932] In the following text, it will discuss how identity disclosure works in civil procedure in China.

6.3.1 Disclosure upon the Order of Courts or Request of Copyright Owners

As being discussed above, in China, besides Copyright Administrations can order identity disclosure, in civil cases, hosting ISPs can also be requested to disclose the suspected infringers' identities. Nevertheless, unlike the relevant rules in the US and EU, the Internet Interpretation (2006) does not specify whether an identity disclosure request from the copyright owner ought to go through judicial examination, which has resulted in a little bit turmoil in judicial practice.

In the case of *Qiao v. tiexue.net*, the defendant ran a website "tiexue.net" which allowed its users to upload pictures on it, and the plaintiff Qiao found some of his copyrighted pictures were uploaded to tiexue.net without permission, so Qiao sued the defendant for copyright infringement.[933] Before the term of adducing evidences expired, the defendant did not submit the registration information of Internet users who uploaded the infringing pictures, so the court held it as a reason to conclude the defendant liable.[934] In another case, the same plaintiff Qiao sued the website china.com for copyright infringement based on the similar facts as in the previous case.[935] During the hearing, the defendant submitted the registration information of Internet users who were alleged to commit copyright infringement, and the court held that the defendant fulfilled its duty of disclosing the infringers' identities.[936] In these two cases, the hosting ISPs disclose the identity information of the suspected infringing users in front of judicial review.

By contrast, there are still some cases where hosting ISPs disclosed their Internet users' identities directly upon the request of the copyright owners. In the case of *3rd Mian Xiang v. Great Wall Broadband*, the defendant Great Wall Broadband provided

932 Internet Interpretation (2006) (网络解释(2006)) (n145), Art. 5.

933 *Qiao v. tiexue.net (乔某某 v. 铁血网)*, Beijing Haidian District Court (北京市海淀区基层人民法院), (2006) Hai Min Chu Zi, No. 15350 (（2006）海民初字第15350号)

934 Ibid.

935 *Qiao v. china.com (乔某某 v. 中华网)*, Beijing Second Intermediate People's Court (北京市海淀区中级人民法院), (2006) Er Zhong Min Chu Zi, No. 8997 (（2006）二中民初字第8997号).

936 Ibid.

webhosting services, and the plaintiff[937] found that some of its copyrighted books were unlawfully available on a website hosted by the defendant, so the plaintiff sued Great Wall Broadband for copyright infringement.[938] In this case, even before filing a lawsuit, the plaintiff sent the defendant a notice which requested the defendant to disclose its client's registration information in question, and then the defendant submitted the corresponding registration information to the plaintiff.[939] Eventually, the court held that the defendant fulfilled its obligation of disclosing the suspected infringing users' identity.

Since the registration information may reveal the identities of Internet users which should be protected as their privacy, any request about disclosing registration information is supposed to be reviewed by the court so as to prevent the abuse of this disclosing procedure. In fact, People's Supreme Court also realizes that any disclosure of information relevant to personal identities needs to be ordered by courts. For instance, in another Judicial Interpretation about protecting rights of person on the Internet, it is clearly prescribed that a People's Court, based on the plaintiff's claim and concrete circumstances in the case, may order the ISP to submit the court the information that can identify the Internet users suspected of infringement, such as their name, contacts, IP addresses and etc.[940] Therefore, the procedural defect stated above may be fixed by People's Supreme Court in the near future.

202 ### 6.3.2 To What Extent Hosting ISPs Ought to Conduct Identity Disclosure

Before "real-name registration" policy was implemented in China,[941] Internet users usually do not need to register for hosting ISPs' services by submitting their real identity information, so the identity information disclosed by hosting ISPs normally cannot have the suspected infringers identified. In a case (*Qiao v. china.com*) discussed above, the registration information disclosed by the defendant just included the so-called internet names such as "wolf", "keer" and "axjidy", and the e-mail addresses,[942] which could not really help the plaintiff identify the real infringers. Nevertheless, the court still held that the hosting ISPs fulfilled the obligation to conduct identity disclosure.

937 In this case, the plaintiff is a copyright agency company, and it got authorization to sue infringers from copyright owners whose books were unlawfully transmitted in question.

938 *3rd Mian Xiang v. Great Wall Broadband (三面向诉长城宽带)*, Hubei Wuhan Intermediate People's Court (湖北省武汉市中级人民法院), (2009) Wu Zhi Chu Zi, No. 18 ((2009) 武知初字第18号).

939 Ibid.

940 Internet Provisions (网络规定) (n208), Art. 4.

941 "real-name registration (网络实名制)" means that when Internet users register for ISPs' services, they need to provide their real identity information. According to Article 6 of Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection (全国人民代表大会常务委员会关于加强网络信息保护的决定), When processing website access services, or landline or mobile phone network access formalities, or providing information release services for users, network service providers shall require the users to provide real identity information when entering into agreements with the users or when confirming the provision of such services. After then, blogs, BBS and other hosting services has started to implement "real-name registration" policy.

942 *Qiao v. china.com (乔某某 v. 中华网)*, Beijing Second Intermediate People's Court (北京市海淀区中级人民法院), (2006) Er Zhong Min Chu Zi, No. 8997 (（2006）二中民初字第8997号).

In the case of *joy.cn v. tudou.com*,[943] the court discussed to what extent should a hosting ISP conduct identity disclosure. In this case, the plaintiff found a TV series copyrighted by it was uploaded to the defendant's website by an Internet users named as "Mo Daqian (莫大千)", so besides suing the defendant for contributory infringement, the plaintiff also requested the defendant to disclose the Internet user Mo Daqian's real name, address, phone number, email address and the IP address used for uploading the TV series. However, during the hearing, the defendant merely provided Mo Daqian's registration information and IP address, which was not sufficient to have Mo Daqian identified. Finally, the court held that the defendant had already fulfilled the obligation of identity disclosure based on the following reasons: (1) it was unreasonable to require the hosting ISPs to disclose more identity information than those provided by its users when registering the accounts; (2) the defendant had proved that the registration information disclosed by it was true. Therefore, if Internet users do not need to register accounts by submitting their real identity information, in most cases, the registration information retained by hosting ISPs normally cannot reveal the real identities of Internet users.[944]

Nevertheless, it is still possible for copyright owners to get sufficient identity information from hosting ISPs in some occasions. In a case (*3rd Mian Xiang v. Great Wall Broadband*) discussed above, the registration information disclosed by the defendant included the client's real name, personal ID number and even the address, which is far enough for the plaintiff to identify the direct infringer.[945]

Based on the above case law, it can be found, regarding to what extent identity information should be disclosed, the Chinese courts only require hosting ISPs to disclose the identity information concerned within its capacity permitted by the Internet technologies, such as the users' registration information. If the identity information disclosed by a hosting ISP is not sufficient to have the suspected infringers identified, so long as it can prove that it has already disclosed the identity information concerned within its capacity permitted by the Internet technologies, it does not violate the obligation of identity disclosure. After the implementation of "real-name registration" policy, Internet users need to register for services with their real identity information, so hosting ISPs are supposed to provide the information which is capable of having alleged infringing users identified.[946]

943 *joy.cn v. tudou.com (激动网v.土豆网)*, First People's Intermediary Court of Shanghai (上海市第一中级人民法院), (2009) HuYiZongMinWu(Zhi)ZhongZi No. 79 ((2009)沪一中民五(知)终字第79号).

944 In the other two disputes between joy.cn and toudou.com, the defendant toudou.com even failed to disclose the alleged infringing users' registration information because these information has been lost, and the courts still held toudou.com fulfilled its obligation of identity disclosure. See Cases: *joy.cn v. tudou.com (*激动网*v.*土豆网), First People's Intermediary Court of Shanghai (上海市第一中级人民法院), HuYiZongMinWu(Zhi)ZhongZi No. 53 ((2009)沪一中民五(知)终字第53号); joy.cn v. tudou.com (激动网v.土豆网), First People's Intermediary Court of Shanghai (上海市第一中级人民法院), HuYiZongMinWu(Zhi)ZhongZi No. 102 ((2009)沪一中民五(知)终字第102号).

945 *3rd Mian Xiang v. Great Wall Broadband (三面向v.长城宽带)* (n933).

946 After the implementation of a"real-name registration" policy, there is still no case in which copyright owners request hosting ISPs to disclose Internet users' identity information. The possible reason might be that it is inefficient to sue Internet users.

6.3.3 Summary in China

In general, China has not set a strict procedure on the disclosure of Internet users' identity information. In most cases, the Internet users' identity information was disclosed by the orders of the courts. However, according to some court decisions of the past, hosting ISPs may directly disclose their users' identity information upon the request of the copyright owners without judicial review. Regarding to what extent should identity information be disclosed, the Chinese courts only require hosting ISPs to disclose the identity information concerned within its capacity permitted by the Internet technologies, such as the users' registration information. Further, like the US, there is no specific rule to require hosting ISPs to retain Internet users' online communication data at legislative level.

As mentioned, in the latest Judicial Interpretation on online copyright infringement, the clause about identity disclosure has been abandoned.[947] Therefore, currently there exists no specific provision regulating identity disclosure in online copyright infringement cases. How does the abandonment of the identity disclosure clause impact upon the judicial practice? Does it mean copyright owners cannot request hosting ISPs to disclose the alleged infringers' identity in copyright cases, or copyright owners still can make the requests as such? After the enactment of the latest Judicial Interpretation, no online copyright case has dealt with the request of disclosing the alleged infringers' identity information.[948] Hence, there is still no clear answer to the questions raised before.

6.4 Comparison of Hosting ISPs' Duties in Identity Disclosure Mechanisms

From the discussion done above, one can find, in the US, EU and China, hosting ISPs can be requested to disclose the Internet users' identity data they have for purpose of fighting against copyright infringement. In the US and EU, copyright owners can only request the hosting ISPs to disclose the Internet users' identity data by applying for the orders from courts. However, in China, hosting ISPs may directly send the Internet users' identity data to copyright owners upon their request, and no judicial review is needed. Regarding data retention, in the US and China, there is no specific rule that requires hosting ISPs to retain their users' communication data. In the EU, although the Data Retention Directive has been enacted to require ISPs to retain their users' communication data, generally the ISPs indicated in this Directive do not cover hosting ISPs.

Despite the existence of these differences, according to the above exploration of identity disclosure mechanisms in the US, EU and China, hosting ISPs' duties can mainly be summarized as answering the following two questions: (1) under what circumstances

947 Internet Provisions (网络规定) (n208). According to the last Article of this Judicial Interpretation, it replaces the Internet Interpretation (2006).

948 A search on the website of "Judicial Opinions of China" on which the judicial decisions are published, did not reveal any case involving identity disclosure in the case of online copyright infringement after the enactment of the latest Judicial Interpretation. See http://www.court.gov.cn/zgcpwsw/, (last visited, August 6, 2015).

can hosting ISPs disclose Internet users' identity information; (2) to what extent should hosting ISPs disclose Internet users' identity information. In the following text, how to answer these two questions will be discussed.

6.4.1 The Pre-conditions of Identity Disclosure

In the light of identity disclosure mechanisms, hosting ISPs are obligated to disclose Internet users' identity information upon requests from competent third parties. Therefore, the obligations undertaken by hosting ISPs are passive rather than active in identity disclosure mechanisms. In the US, EU and China, competent authorities can order hosting ISPs to disclose such information to them. Nevertheless, regarding how copyright owners can get alleged infringers' identity information, different approaches have been adopted in the US, EU and China. In the EU, normally, copyright owners need to launch lawsuits, and request courts to order hosting ISPs to disclose alleged infringers' identity information to them.[949] In the US, although the applications of identity disclosure also have to be submitted to courts, disclosure subpoenas are issued by clerks with no need of judges' approval,[950] so identity disclosure can be ordered without sufficient examination.[951] In China, Internet users' identities can even be passed on to copyright owners without judicial review.[952]

Since identity disclosure is relevant to the protection of Internet users' privacy, hosting ISPs should conduct identity disclosure by following due process. Nevertheless, because of anonymity on the Internet, the clash between copyright protection and privacy security has come to the fore.[953] Some scholars even argue that the protection of copyright endangers privacy.[954] In order to properly define hosting ISPs' duties in protecting Internet users' privacy, it is necessary to explore the reasons resulting in privacy concerns of identity disclosure. First, identity information can be disclosed without judicial review, and for the purpose of avoiding liability, hosting ISPs tend to disclose their users' identity information upon copyright owners' request without taking into account privacy protection (China). Second, disclosure subpoenas can be issued by clerks without sufficient examination (the US). In the case of Wal-Mart, in order to acquire the identity of the person who posted "Wal-Mart Day After Thanksgiving sales

949 Kuner C, et al., Study on online copyright enforcement and data protection in selected Member States (n895).

950 David Gorski, *Future of the Digital Millennium Copyright Act (DMCA) Subpoena Power on the Internet in Light of the Verizon Cases, The*, 24 Rev. Litig. (2005). 158. In terms of DMCA 512(h), the subpoena can be ordered by a clerk rather than a judge.

951 Bretan, 'Harboring Doubts about the Efficacy of 512 Immunity under the DMCA' (n49), at 52-53. Katyal, 'Privacy vs. Piracy' (n25), at 330.

952 *3rd Mian Xiang(三面向诉长城宽带) v. Great Wall Broadband* (n933).

953 Vincents OB, 'When rights clash online: The tracking of P2P copyright infringements vs. the EC personal data directive' (2008) 16 International Journal of Law and Information Technology 270, at 270.

954 Cohen, 'Overcoming Property: Does Copyright Trump Privacy?' (n40), at 101. Katyal, 'Privacy vs. Piracy' (n25), at 335 and 345. Edwards, 'Should ISPs be Compelled to Become Copyright Cops? File-Sharing, the Music Industry and Enforcement Online' (n40).

information" on the FatWallet site, Wal-Mart applied for a subpoena under DMCA § 512(h) by "submitting a declaration under penalty of perjury that its sales prices were protected by copyright law," and the federal court approved such a ridiculous application.[955] Third, a copyright owner can request the subpoena to disclose someone's identity without submitting substantial evidence about infringement (the US).[956] In light of DMCA 512 (h), when applying for a subpoena, a copyright owner only needs to submit a copy of a notice, a proposed subpoena and a sworn declaration that the identity is acquired for the purpose of protecting its copyright, but no evidence about copyright infringement is necessary.[957]

Among these three reasons, hosting ISPs are only responsible for the first one. Therefore, in order to solve privacy concerns of identity disclosure mechanism, hosting ISPs' duties are to refrain from disclosing Internet users' identity information to copyright owners without orders from courts. By contrary, the positive duties ought to be imposed on courts and copyright owners, such as copyright owners are obligated to submit sufficient evidences about infringement when applying for disclosure orders, and courts ought to examine the applications in a diligent way.

6.4.2 Disclosing Obligations of Hosting ISPs

Once receiving disclosure orders from competent authorities, hosting ISPs are obligated
206 to disclose Internet users' identity information. Nevertheless, when Internet users register for hosting ISPs' services, they normally do not need to submit their real identity information (except in China). Therefore, usually hosting ISPs do not keep the sufficient information which is capable of having the suspected infringers identified. Under this condition, even if hosting ISPs are obligated to disclose the identity information they retain, the suspected infringers still fail to be identified.

China offers a solution for this problem, and that is to force hosting ISPs to require their users to submit the real identity information when registering for the services. However, this solution can hardly be copied in the EU and US. First, it would impose the costly burden on hosting ISPs, since the hosting ISPs need to examine the identity information provided by Internet users and make sure these identity information is real, but such a duty may run beyond the capacity of hosting ISPs. More importantly, it goes against enlarging Internet users' freedom of speech, if requesting Internet users to submit their real identity information. In cyberspace, anonymity is considered to play an important role in guaranteeing the freedom of expression, because anonymity not only allows the public to freely deliver their opinions about "their interests, beliefs and political ideologies without fear of reprisals from the state or any other powerful organization," but

955 Gray ME, *FatWallet Victorious in Challenge to Wal-Mart's Frivolous DMCA Subpoena*, BerkleyLaw(2002), *available at* http://www.law.berkeley.edu/4719.htm (last visited 20-08-2014).

956 DMCA (n1) Sec. 512 (h).

957 Ibid.

also "permits others to receive these views."[958] Compared with China, the EU and US obviously attach more importance to protecting citizen's freedom of speech, and the "real-name registration" policy therefore can hardly be an option for the EU and US.
Another solution might be to require hosting ISPs to retain Internet users' online communication data. Nevertheless, so far the US and China have not enacted the regulation on data retention at legislative level. Particularly, in the US, There were several bills which aimed at requiring ISPs to retain online data, but because of privacy concerns, eventually all of them failed to become law.[959] In the EU, the Data Retention Directive has been enacted for fighting against serious crimes rather than copyright infringement, and hosting ISPs are not obligated to conduct identity data retention according to the Article 5 of the Directive.[960] In addition, because of the serious privacy concerns on data retention, in 2014, the ECJ held the Data Retention Directive disproportionate, even though this directive was enacted for public good – against serious crimes.[961] Therefore, currently there is no strong reason to justify the obligation that requires hosting ISPs to retain Internet users' online communication data for copyright enforcement.

6.5 Conclusion

In the US, EU and China, hosting ISPs are all obligated to disclose Internet users' identity information under certain circumstances. In the US and EU, hosting ISPs are only subject to disclosing orders from competent authorities, and if a copyright owner wants to acquire the identity of an alleged infringer, it needs to request the court to issue an identity disclosure order. By contrast, in China, there is not specific procedure to regulate the identity disclosure in civil disputes, and hosting ISPs may even disclose Internet users' identity information to copyright owners upon their request. Although the disclosure of personal identity is to a certain degree necessary for the purpose of copyright enforcement on the Internet, it also may put Internet users' privacy in danger. Therefore, due process should be rendered on the disclosure of identity. From the perspective of hosting ISPs, they are not the initiators but just reactors of this mechanism, so they only need to fulfill a passive obligation which is not to voluntarily communicate their users' identity information to copyright owners without orders from courts or competent authorities. In addition, hosting ISPs are only obligated to disclose the identity information retained by them. However, the personal data retained by hosting ISPs may not be sufficient to have the suspected infringers identified, so the effectiveness of identity disclosure is in question. In China, this problem has been solved by adopting

958 Williams, 'On-Line anonymity, deindividuation and freedom of expression and privacy' (n41), at 687.
959 United States, Electronic Frontier Foundation, (n885).
960 Feiler, '*The legality of the data retention directive in light of the fundamental rights to privacy and data protection*' (n906).
961 See *Digital Rights Ireland Ltd v Minister for Communications and others* (n911).

"real-name registration" policy. Nevertheless, similar policy can hardly be transposed into the US and EU because of concerns on freedom of speech. Moreover, it is also inappropriate to require hosting ISPs to retain Internet users' online communication data because of privacy concerns.

To sum up, in identity disclosure mechanisms, even though information disclosed by hosting ISPs are not sufficient to have alleged infringers identified, hosting ISPs should be still held to fulfill their duties if they have disclosed the identity information retained by them. Further, because privacy is protected as a fundamental right, hosting ISPs shoulder an obligation of omission which is to refrain from disclosing identity information to copyright owners without court orders. These duties are easy for hosting ISPs to fulfill, and do not negatively affect hosting ISPs' freedom to operate in the US, EU and China.

Chapter 7

Self-regulation of Copyright Enforcement on Hosting Platforms

Introduction:

Since the birth of the Internet, some scholars have been prompting the idea that the Internet should not be subject to traditional forms of governance, and self-regulation or self-governance is more proper to solve the problems in the Internet.[962] In the digital realm, it's nearly impossible for traditional forms of governance to keep pace with the rapid development of digital technologies, and the specialized legal rules "would likely become outdated shortly thereafter".[963] Therefore, the self-regulation which is more flexible and easier to update, can play an important role in cyberspace.[964] Besides, even with the application of state regulation, the copyright infringement on the Internet still has not been reduced to a tolerable level, for which self-regulation needs to coexist with state regulation.[965] Further, the state regulation also admits the positive impact of self-regulation. For example, the E-Commerce Directive encourages trade, professional and consumer associations or organizations to draw up codes of Conduct at community level so as to better implement the Directive.[966] What occurs in digital copyright enforcement also demonstrates the importance of self-regulation. As noted by Prof. Hugenholtz, traditionally, courts take charge in copyright enforcement, either in civil procedures or criminal procedures; however, on the internet, "copyright enforcement is gradually being moved from the courts and put into the hands of intermediaries applying a self-imposed 'code of conduct'".[967] It is a global tendency that ISPs are either committing or compelled to commit themselves to self-regulatory rules and procedures which aim at solving massive copyright infringement on the Internet.[968]

Basically, the self-regulation regarding hosting ISPs can be divided into two categories, one of which is the code of conduct achieved among multiple stakeholders,[969] and the other one is the so-called "second level agreements"[970] reached between copyright owners and hosting ISPs. Since it is common that the contents uploaded to hosting platforms contain materials owned by copyright owners, hosting ISPs reach second level agreements with copyright owners so as to decide how to deal with these suspected infringing contents from a business perspective. Over time, second level agreement

962 Johnson DR and David G, 'Post, Law and Borders: The Rise of Law in Cyberspace' (1996) 48 Stanford Law Review 1367, at 1370. Gibbon LJ, 'No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace' (1996) 6 Cornell Journal of Law and Public Policy 475. Hardy IT, 'The Proper Legal Regime for Cyberspace' (1993) 55 University of Pittsburgh Law Review 993.

963 Easterbrook FH, 'Cyberspace and the Law of the Horse' (1996) 1 University of Chicago Legal Forum 207, at 213.

964 Hugenholtz, 'Codes of Conduct and Copyright Enforcement in Cyberspace' (n55), at 305.

965 Anon, 'The Principles for User Generated Content Services: A Middle-Ground Approach to Cyber-Governance' (2008) 121 Harvard Law Review 1387, at 1406.

966 E-commerce Directive (n1), Art.16.

967 Hugenholtz, 'Codes of Conduct and Copyright Enforcement in Cyberspace' (n55), at 303.

968 Ibid.

969 For instance, the Principles for User Generated content services (n42).

970 The Second level agreement is a term used by Yafit Lev-Aretz. According to her definition, a second level agreement is a pre-emptive license obtained by hosting ISPs to ratify the mass usage of copyrighted materials by their users. See Lev-Aretz Y, 'Second Level Agreements' (2011) 45 Akron Law Review 137, at 152.

became "more standardized"[971], and thus reflects the "deference to the cross-industry form of private ordering"[972]. Generally, Codes of Conduct tend to focus on how should the ISPs and copyright owners cooperate together to reduce the infringement, but second level agreements also contribute to "ratify[ing] the mass usage of copyrighted materials" on hosting platforms.[973]

According to the norms set in these self-regulation document, hosting providers need to assume some responsibilities which are not prescribed in legislation or case law for the purpose of reducing copyright infringement. This chapter analyzes the responsibilities indicated in these two types of self-regulation, and then evaluates how they affect hosting ISPs' freedom to operate when solving the copyright disputes on hosting platforms. It starts with the discussion on codes of conduct (7.1). In this part, according to the variety of involving intensities from government, it explores the norms set in three different codes of conduct, which are Notice-and-Takedown Code of Conduct (hereafter NT Code), Principles for User Generated Content Services (hereafter UGC Principles), and Self-discipline Codes in China. Based on the exploration done on these three codes of conduct, it evaluates the codes of conduct from the perspective of preserving hosting ISPs' freedom to operate by comparing them with state regulatory norms (7.1.4). In the next section (7.2), it discusses the second level agreements reached between copyright owners and hosting ISPs. First, it explores the substantial contents of second level agreements (7.2.1). Then, it evaluates the advantages and disadvantages of second level agreements in respect of preserving hosting ISPs' freedom to operate (7.2.2 and 7.2.3). Finally, it answers the question – whether self-regulation can better regulate hosting ISPs' copyright responsibilities with regard to preserving their freedom to operate (7.3).

7.1 Codes of Conduct

Codes of conduct are the agreements achieved between multiple stakeholders so as to solve the copyright infringement problem in hosting services. From the perspectives of stakeholders, they need such kind of codes of conduct for their own interests. For example, copyright owners would like to ask hosting ISPs to take more responsibility in reducing the infringement. From the perspective of hosting ISPs, they are also willing to take more copyright-protecting measures so as to get the copyright owners' promises of not suing in return. Besides, governments also prefer to see the stakeholders solve the tremendous copyright infringement on the Internet by themselves, so they can save lots of time and energy in law-making.[974] Normally, codes of conduct mean the norms

971 Ibid.

972 Lev-Aretz Y, 'Copyright Lawmaking and Public Choice: From Legislative Battles to Private Ordering' (2013) 27 Harvard Journal of Law & Technology 203, at 251.

973 Lev-Aretz, 'Second Level Agreements' (n965), at 152.

974 Hugenholtz, 'Codes of Conduct and Copyright Enforcement in Cyberspace' (n55), at 304.

resulting from self-regulation committed by private actors, but the authorities also often participate in the norms-setting process under a self-regulatory framework in varying degrees of intensity,[975] such as the Notice-and-Takedown Code of Conduct in the Netherlands.[976] However, there are still some codes of conduct purely achieved among private entities, such as Principles for User Generated Content Services.[977] In China, government even plays a dominant role in drafting the self-regulation norms, such as "Self-discipline Treaty on Internet Audio-video Program Services in China" (hereafter Self-discipline Treaty) and "Self-discipline Declaration on Copyright Protection by the Internet Industry in China" (hereafter Self-discipline Declaration).[978] In the following text, these four codes of conduct will be analyzed.

7.1.1 NT Code of Conduct

At the EU level, the E-Commerce Directive does not codify the notice-and-takedown procedure, but Member States are encouraged to explore this procedure at their own discretion.[979] In the Netherlands, with the efforts from governmental sectors and private entities (especially copyright owners and ISPs), a code on notice-and-takedown procedure was achieved in 2008 so as to deal with the illegal content on the Internet. The code has 7 Articles, which provide detailed rules about the notice-and-takedown procedure, including the requirement of notice, the evaluation done by ISPs and the corresponding measures after the evaluation.

214

7.1.1.1 Requirement of Notice

The Code first clarifies that the notifier should be responsible for the accuracy of the notices, and then the Code differentiates the notices sent from public authorities and private sectors.[980] Regarding the notices sent by public authorities in formal investigating processes, such as a notice from the Public Prosecutor's Office with an imperative character, the Code does not set any particular requirement on the content of such notices, and the ISPs are obliged to comply with them.[981]

975 Ibid.

976 *Notice-and-Take-Down Code of Conduct*, ecp.nl (2008), *available at* http://ecp.nl/over-ecp/216/over-ecp.html (last visited 15-12-2014).

977 Principles for User Generated Content Services (n42).

978 In the case of Self-discipline Treaty, it was drafted and published by the State Administration of Radio Film and Television for the industry participants to sign in. see *Self-discipline Treaty on Internet Audio-video Program Services in China (中国互联网视听节目服务自律公约)* (n42). Regarding the Self-discipline Declaration, without the active coordination done by National Copyright Administration and Beijing Municipal Bureau of Copyright, it is almost impossible that more than 100 websites would sign in this Declaration. See *101 websites sign in "Self-discipline Declaration on Copyright Protection by Internet Industry in China" together (101家网站共同发布《中国互联网行业版权自律宣言》)*, www.npc.gov.cn (全国人大网)(2010), *available at* http://www.npc.gov.cn/npc/xinwen/fztd/fzsh/2010-01/21/content_1535617.htm (last visited 12-12-2014).

979 Directive 2000/EC/31, Art. 21.2, this Article requires the Commission to submit a report about notice-and-takedown procedure, so this procedure is definitely encouraged by the E-Commerce Directive.

980 Notice-and-Take-Down Code of Conduct (n971), Art. 4.

981 Ibid, Art. 4a and Note to Art. 4a.

However, if a notice is sent from the private sector, it should contain the following information:[982]

1) The contact details of the notifier;

2) The information that the intermediary needs to be able to evaluate the content, at least including the location (URL);

3) A description of why the content is unlawful according to the notifier, or why it is in conflict with the criteria published by the intermediary governing undesirable content;

4) A statement of reason why this intermediary is being approached as the most appropriate intermediary to deal with the matter.

After checking the elements listed above, it can be seen that the Code sets a quite strict requirement on the content of a competent notice. In a competent notice, the copyright owner not only needs to indicate the location of the alleged infringing materials as precisely as possible,[983] but also demonstrates why the alleged infringing materials are unlawful or undesirable content. Besides, copyright owners can also request the urgent removal of infringing materials indicated in the notices, but sufficient reasons need to be given to explain why an urgent removal is necessary.[984] For instance, in the case of dealing with repeated infringement, a request for urgent remove can be initiated.[985]

7.1.1.2 Evaluation of Notice

After receiving a notice from a copyright owner, the ISP need not comply with the notice automatically, but should evaluate the notice and then decide whether the materials complained in the notice are unlawful or undesirable.[986] Nevertheless, the Code does not set a standard about the evaluation, and ISPs can make their own evaluating policies. Therefore, ISPs can choose to undertake a superficial or sophisticated evaluation.

7.1.1.3 Measures to Be Taken

After the evaluation, the ISPs can take different measures based on their evaluation result in each case. If an ISP concludes that the designated materials are not

982 Ibid, Art. 4b.
983 Ibid, Note to Art. 4b.
984 Ibid, Art. 4c.
985 Ibid, Note to Art. 4c.
986 Ibid, Art. 5.

unequivocally unlawful, it should inform the notifier about its conclusion with the reasons attached.[987] But if an ISP concludes that the materials are unequivocally unlawful, the ISP should immediately remove the materials.[988] In the event that an ISP cannot be quite sure about whether the complained materials are unlawful or not, the ISP should forward the notice to the person who provided the materials concerned.[989] After receiving the notice forwarded by the ISPs, the content providers need to contact the corresponding notifiers, and discuss how to deal with the content.[990] If an agreement cannot be reached between notifier and content provider, the notifier can either make an official notice to the police, or launch a lawsuit against the content provider. However, in practice, content providers may not contact the notifiers even after receiving the notices forwarded by the ISPs, and in this situation, the ISPs may either take the content offline, or disclose the content providers' identities, such as content providers' name, contact information.[991] Besides, the ISPs should undertake due caution to prevent any mistaken removal.[992]

7.1.1.4 Assessment

Comparing with the codified notice-and-takedown procedures discussed in the previous chapter, the procedure set in the Code is more detailed and clear for the relevant parties to fulfill their obligations.[993] In this regard, hosting ISPs face more
216 legal certainty in the procedure. In addition, the Code also includes several flexible provisions. As discussed above, ISPs need to evaluate notices with due caution, but notifiers are responsible for the accuracy of notices. Therefore, ISPs can in fact define the "due caution" by themselves, which avoids imposing unreasonable evaluation burden on them.[994] Further, the Code allows hosting ISPs and copyright owners to make further mutual arrangements between them. As indicated in Note to Art. 7c, copyright owners and ISPs are free to collaborate with each other to speed up the whole procedure.[995] For example, a notifier can be regarded as a trusted party so that the evaluation of its notices can be omitted.[996] With these flexible

987 Ibid, Art. 6a.
988 Ibid, Art. 6b.
989 Ibid, Art. 6c.
990 Ibid.
991 Ibid, Note to Art. 6c.
992 Ibid, Art. 6d.
993 Besides including 7 detailed Articles that regulate notice-and-takedown procedure, the Code also provides explanatory notes to these Articles. These explanatory notes instruct how to interpret each Article in different circumstances, which helps to clarify relevant parties' duties in the procedure.
994 In Section 5.5, the author demonstrates that it is too burdensome for hosting ISPs to evaluate notices so as to ensure their accuracy, so hosting ISPs should not be obligated to conduct such evaluation. By contrast, in the context of self-regulation, the intensity of evaluation (due caution) can be defined by ISPs themselves, which can avoid imposing unreasonable burden on ISPs while encouraging them to evaluate notices based on their capacity.
995 Ibid. Note to Art. 7c.
996 Ibid.

arrangements, ISPs have more freedom to decide their anti-piracy policies during operation. Further, the Code is not a binding contract,[997] and it means that hosting ISPs can choose whether to fulfill the duties prescribed in the Code. Nevertheless, non-bindingness also means that hosting ISPs may still face risk of being sued by copyright owners, even though they fulfill these duties.

7.1.2 Principles for User Generated Content Services

In 2007, in order to solve the overwhelming copyright infringement over the Internet, some copyright giants, such as CBS, Sony and Disney, reached an agreement with some leading hosting ISPs, including Dailymotion and Veol.[998] The Principles admit that no anti-piracy system is perfect, but hosting ISPs need to be more active in eliminating copyright infringement. Particularly, hosting ISPs are required to take some measures which go beyond the statutory requirement, such as employing content identification technologies. In general, UGC Principles can be seen as a win-win deal when statutory law fails to properly solve the copyright infringement on the Internet, because according to UGC Principles, hosting ISPs promise to take more efficient measures to eliminate infringement in exchange for the not-suing promise from copyright owners.

At the beginning of UGC Principles, the objectives pursued by parties are enumerated as follows: (1) eliminating infringing content on UGC websites; (2) encouraging the upload of original and authorized user-generated content; (3) accommodating fair use on UGC websites; (4) protecting the legitimate interests of user privacy. Besides listing these general objectives which are about balancing all involved interests, UGC Principles require hosting ISPs to adopt content identification technologies which aim at eliminating copyright infringement on their platforms.

Content identification technologies allow hosting ISPs to identify whether the materials uploaded by Internet users contain any content copyrighted by any signee of UGC Principles. In order to fulfill this goal, copyright owners should first offer "the reference data for content to establish a match with user-uploaded content", and then indicate how to deal with the user-uploaded content which matches the reference data.[999] If copyright owners have not indicated any specific treatment for the matched content, this matched content needs to be blocked by hosting ISPs.[1000] Besides blocking matched content from being uploaded, copyright owners can also choose the alternative treatment, such as allowing the content to be uploaded,

997 Ibid, see introduction of explanatory statement, and it states "complying with the code is voluntary, and there can be no formal enforcement in the case of non-compliance."

998 *Internet and Media Industry Leaders Unveil Principles to Foster Online Innovation While Protecting Copyrights*(2007), *available at* http://www.ugcprinciples.com/press_release.html.

999 Principles for User Generated Content Services (n42), Art. 3a.

1000 Ibid.

licensing use of the content, etc..[1001] From the perspective of hosting ISPs, they first should establish databases used for filtering out matched content, and make it reasonably convenient for copyright owners to deliver the reference materials to the filtering database.[1002] Further, before any up-loaded content can be made available on hosting ISPs' websites, it needs to pass through the filtering database, and if any user-uploaded content matches the reference materials, the hosting ISP needs to take corresponding measures, such as blocking or other measure indicated by copyright owners.[1003] Besides, hosting ISPs can manually review all of the user-uploaded content as a complement or replacement to content identification technology, so long as the manual review is as effective as the identification technology in terms of eliminating infringing content.[1004] With the purpose of avoiding blocking any authorized content, copyright owners should provide a list of users authorized to utilize the content which would match the reference materials.[1005]

In order to ensure that content identification technologies function properly, when copyright owners deliver the reference materials to the hosting ISPs, they should "believe in good faith that they have the appropriate rights to do so, and update rights information as reasonable to keep it accurate."[1006] Besides, copyright owners should coordinate with hosting ISPs so as to avoid unduly stressing the content identification technology, such as delivering too much reference material during limited periods.[1007] Further, with the cooperation from copyright owners, hosting ISPs should reasonably ensure that these reference materials are incorporated into the content identification system as soon as possible in such overload periods.[1008] Because infringing content might be uploaded before the corresponding reference materials are incorporated into the content identification system, hosting ISPs should regularly use the content identification system to check throughout their service and then remove such infringing materials.[1009] In order to protect users' legal interests while preventing infringement, a reasonable procedure should be developed by copyright owners and hosting ISPs to deal with the case where users and copyright owners have conflicting claims over the content which is blocked or removed by the content identification system.[1010]

Besides establishing a content identification system, UGC Principles also ask hosting ISPs to undertake some other duties which go beyond statutory obligation.

1001 Ibid, Art. 3c.
1002 Ibid, Art. 3a.
1003 Ibid, Art. 3c.
1004 Ibid, Art. 3f.
1005 Ibid, Art. 3e.
1006 Ibid, Art. 3g.
1007 Ibid.
1008 Ibid.
1009 Ibid, Art. 3h.
1010 Ibid, Art. 3i.

First, hosting ISPs should work with copyright owners to identify the sites which are "dedicated to, and predominately used for" infringement, or facilitating such infringement. Once such a site has been identified, the hosting ISP must block the links to this site, and if the hosting ISP is able to identify specific links which solely offer access to legal content on such site, the hosting ISP may not block these legal links.[1011] Second, hosting ISPs should provide commercially reasonable means to help copyright owners locate the infringing content throughout their websites where user-uploaded content is publicly accessible.[1012]

UGC Principles also reiterate some rules which have been provided in current law, but make these rules more detailed. First, hosting ISPs should in relevant and conspicuous places on their sites state that they promote the respect for intellectual property rights and discourage infringing content from being uploaded, and also inform users not to upload any infringing content.[1013] Second, when copyright owners send notices to hosting ISPs, the notices should include the URLs by which the hosting ISPs can locate the infringing content.[1014] After receiving a notice, the hosting ISP needs to expeditiously remove the corresponding content, notify the uploader, and if the uploader sends a qualified counter-notification, the hosting ISP should forward this counter-notification to the relevant copyright owner.[1015] These measures just mirror notice-and-takedown procedure in DMCA 512.[1016] However, as for whether to replace the removed content, UGC Principles indicate a different solution, which is that hosting ISPs can decide at their own option, to follow either applicable law or the agreement with copyright owners.[1017] Besides, UGC Principles also reinforce the repeat infringer termination policy provided in DCMA 512.[1018] According to UGC Principles, in order to properly implement the repeat infringer termination policy, hosting ISPs should take reasonable measures to track the infringing uploads from the same user, and prevent the terminated user from applying for a new account by reusing the verified email address.[1019] Further, measures also need to be taken against repeat infringing content. After infringing content has been removed as requested by a notice, the copyright owner can either do it by itself or request the hosting ISP to incorporate the infringing content into the content identification system as reference data.[1020]

According to UGC Principles, hosting ISPs also have a duty to retain user's online

1011 Ibid, Art. 4.
1012 Ibid, Art. 5.
1013 Ibid, Art. 1, 2.
1014 Ibid, Art. 7.
1015 Ibid, Art. 8.
1016 See DCMA (n1), Sec. 512, c(1)(C), g(2)(A) and g(2)(B).
1017 Principles for User Generated Content Services (n42), Art. 8.
1018 See DMCA (n1), Sec. 512, i(1)(A).
1019 Principles for User Generated Content Services (n42), Art. 11.
1020 Ibid, Art. 9.

communication data for 60 days, and copyright owners can request this data in terms of law, when this data is necessary for any valid process.[1021] This data includes: "(a) the information related to user uploads of audio and video content to their services, including Internet Protocol addresses and time and date information for uploaded content; and (b) user-uploaded content that has been on their services but has been subsequently removed following a notice of infringement."[1022] This data will help immensely, when copyright owners try to trace the identities of users who upload infringing materials. For instance, according to DMCA 512(h), copyright owners can apply for subpoenas to request hosting ISPs to disclose the suspect users' identity information, but the hosting ISPs only need to disclose it to the extent that such information is available to them.[1023] However, users usually do not reveal their true identity, when registering accounts for hosting ISPs' services, so the hosting ISPs might not keep much information about users' identity. UGC Principles set an obligation for hosting ISPs to retain users' uploading data, which not only makes the identification of users available, but also offers evidence to prove infringement. Compared to the statutory rules, hosting ISPs need to shoulder more duties to reinforce copyright protection on their platforms under the frame of UGC Principles. In the light of the non-monitoring responsibility clause and notice-and-takedown procedure provided in DMCA 512, copyright owners should take the main responsibility to police copyright infringement.[1024] Nevertheless, according to UGC Principles, most of the burden of monitoring copyright infringement is shifted from copyright owners to hosting ISPs.[1025] For instance, content identification technologies need to be adopted by hosting ISPs so as to filter out the infringing content before it is made available on the Internet. By contrast, if following notice-and-takedown procedure, hosting ISPs only need to react correspondingly to notices send by copyright owners. Further, UGC Principles also impose some other duties on hosting ISPs, such as reinforcing repeat infringer policy, preventing the same infringing materials from being uploaded again and retaining users' uploading data.

7.1.3 Self-discipline Code in China

In China, several self-discipline codes about copyright enforcement on the Internet have been reached in the past decade, and the administrative agencies always take a lead in drafting and promoting these codes. For example, "Self-discipline Treaty on Internet Audio-video Program Services in China" (hereafter Self-discipline Treaty) was drafted and published by the State Administration of Radio Film and Television

1021 Ibid, Art. 10.
1022 Ibid.
1023 DMCA (n1), Sec. 512, (h).
1024 Ibid.
1025 Anon, 'The Principles for User Generated Content Services: A Middle-Ground Approach to Cyber-Governance' (n960), at 1401.

for the industry participants to sign.[1026] In the case of "Self-discipline Declaration on Copyright Protection by the Internet Industry in China" (hereafter Self-discipline Declaration), without the active coordination done by the National Copyright Administration and Beijing Municipal Bureau of Copyright, it is almost impossible that more than 100 websites would sign this Declaration.[1027]

7.1.3.1 Self-discipline Treaty

The Self-discipline Treaty was drafted by the State Administration of Radio Film and Television which focuses more on censoring the inappropriate content[1028] rather than filtering out infringing content, so anti-piracy is not the main purpose of the Self-discipline Treaty. However, the measures adopted by the Self-discipline Treaty do contribute to copyright protection.

According to Article 4 of the Self-discipline Treaty, the signatories should comply with the laws about regulating the copyright of audio-video programs on the Internet, actively take copyright-protection measures, respect and protect the legal interest of copyright owners and the units offering audio-video program services on the Internet, so as to create and maintain a fair and orderly copyright environment for Internet audio-video programs, and promote the development of the Internet audio-video program service industry.[1029] Besides, the signatories should establish a database for collecting the information about Internet audio-video programs together, and they are also encouraged to notify the other signatories about the audio-video programs which are illegal in terms of laws, statutes, regulations and policies through the foresaid database.[1030] Further, the signatories should regularly log on the database so as to check the illegal contents gathered in the database, and if any of this illegal content is available on their websites, they need to remove it.[1031]

1026 *Self-discipline Treaty on Internet Audio-video Program Services in China (中国互联网视听节目服务自律公约)* (n42).

1027 *101 websites sign in "Self-discipline Declaration on Copyright Protection by Internet Industry in China" together (101家网站共同发布《中国互联网行业版权自律宣言》)* (n973).

1028 There is no standard definition about "inappropriate content", but generally, the following content will be treated as inappropriate: 1) any content that is against the basic principles prescribed and set by the Constitution; 2) any conduct that endangers the unification, the integrity, the sovereignty and the territory of the State; 3) any content that divulges state secrets, endangers national security, or harms the honor and interests of the State; 4) any content that instigates national hatred and ethnic discrimination, undermines national solidarity, or infringes people's walks of life and or customs; 5) any content that propagates paganism or superstition; 6) any content which disturbs social order or undermine social stability; 7) any content that induces minors to cross social lines, violate laws and commit crimes, or exaggerates violence, pornography, gamble, or terrorist activities …, see State Administration of Radio Film and Television; Ministry of Information Industry (国家广播电影电视总局; 信息产业部), Administrative Provisions for the Internet Audio-Video Program Service (互联网视听节目服务管理规定), Order No. 56 of the State Administration of Radio, Film and Television and the Ministry of Information Industry (国家广播电影电视总局、中华人民共和国信息产业部令第56号), December 20, 2007, Art. 16.

1029 *Self-discipline Treaty on Internet Audio-video Program Services in China (中国互联网视听节目服务自律公约)* (n42), Art. 4.

1030 Ibid, Art. 7(2).

1031 Ibid, Art. 7(3).

As referred to above, the database is built mainly for the purpose of filtering out sensitive/inappropriate contents, but since the contents which infringe copyright are part of inappropriate contents, the database can also contribute to copyright enforcement on hosting platforms.

7.1.3.2 Self-discipline Declaration

The Self-discipline Declaration specifically aims at eliminating copyright infringement on the Internet, and it requests hosting ISPs to take more measures than those prescribed in law so as to reduce copyright infringement. As stated by Mr. Zhang (vice chairman of Copyright Society of China), the duties set in the Self-discipline Declaration are not too hard to comply with, but a certain level of effort still needs to be done to fulfill them.[1032]

First, hosting ISPs should reinforce the supervision and management of contents uploaded by Internet users, and deter Internet users from uploading contents copyrighted by others and committing copyright infringement through their Internet platform.[1033] Second, hosting ISPs also need to actively adopt the standard technical measures that are recognized by industries so as to prevent infringement from occurring.[1034] Further, hosting ISPs should particularly take technical measures to restrict the following content from being uploaded, including: 1) the contents cannot be disseminated without permission from competent authorities; 2) the audio-video works that are newly distributed, popular and still on screen.[1035] Therefore, the Self-discipline Declaration sets an obligation for hosting ISPs to monitor the audio-video works that are newly distributed, popular and still on screen. Third, if a user violates service terms, refuses to heed the exhortation, and repeatedly disseminates illegal contents, the hosting ISPs should not only remove corresponding contents and terminate the service to the user, but also report the user to the relevant authorities.[1036] Fourth, hosting ISPs should treat the notices from copyright owners seriously, and ensure that the infringing content will be removed in 24 hours after receiving competent notices.[1037] Fifth, hosting ISPs should actively develop a copyright identification and claim system so as to provide a convenient way for copyright owners to claim their copyright and license their works.[1038] Further, the Internet industry (including hosting ISPs) should actively communicate with

1032 *Press Conference on 2009 Special Action held by State Administration of Press and Publication(新闻出版总署2009专项行动新闻发布会)*, http://www.scio.gov.cn/(2010), *available at* http://www.scio.gov.cn/wlcb/blxxjbygl/Document/527754/527754.htm (last visited 20-12-2014).

1033 Self-discipline Declaration, Art. 3.

1034 Ibid, Art. 4.

1035 Ibid.

1036 Ibid, Art. 5.

1037 Ibid, Art. 6.

1038 Ibid, Art. 7.

copyright owners and relevant associations, and develop the new copyright license mechanism in the online environment so as to promote the legal dissemination of works.[1039]

Like UGC Principles, the Self-discipline Declaration not only crafts some statutory rules, such as repeat infringer policy and action term upon receiving notices, but also sets some new duties for hosting ISPs, such as adopting standard technical measures, monitoring audio-video works which are newly distributed, popular and still on screen, and developing a copyright identification and claim system. In addition, the Self-discipline Declaration also encourages hosting ISPs to develop a new copyright license mechanism with copyright owners.

7.1.4 The Evaluation of the Codes of Conduct

From the self-regulation documents discussed above, a general tendency can be drawn, and that is, compared with state norms, hosting ISPs need to take more responsibilities to eliminate copyrighted contents from being uploaded without permission.[1040] Further, the rules set in self-regulation are more detailed and explicit for copyright owners and hosting ISPs to follow.[1041] In following text, by comparing with state norms, a further examination will be done to self-regulation from the perspective of preserving the freedom to operate of hosting ISPs' copyright.

7.1.4.1 A New "Safe Harbor"

In the context of codes of conduct, hosting ISPs promise to fulfill the duties prescribed in self-regulation. Although these duties may go beyond the obligations set in state norms, hosting ISPs usually can avoid being sued by copyright owners once fulfilling these duties. As provided in Art. 14 of UGC Principles, "If a UGC Service adheres to all of these Principles in good faith, the Copyright Owner should not assert a claim of copyright infringement against such UGC Service with respect to infringing user-uploaded content that might remain on the UGC Service despite such adherence to these Principles."[1042] In this regard, codes of conduct create another kind of "safe harbor" for hosting ISPs.

According to the above discussion on codes of conduct, state of the art filtering technologies have been required to be installed into hosting services, which helps immensely to eliminate copyright infringement. As noted by Lessig, the code is "the most effective way to regulate behavior in cyberspace."[1043] Before any content can be

1039 Ibid, Art. 8.

1040 For example, hosting ISPs are commonly requested to adopt filtering technologies.

1041 Taking notice-and-takedown procedure as an example, the Code of Conduct and UGC Principle clearly request copyright owners to submit the IP addresses of infringing materials in notices, and the Self-discipline Declaration requires hosting ISPs to remove the designated materials in 24 hours after receiving the notices.

1042 Principles for User Generated Content Services (n42), Art. 14.

1043 Lessig L, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 Harvard Law Review 501, at 514.

uploaded and made available on hosting platforms, it needs to pass the inspection done by filtering technologies, so most of infringing uploads cannot ever be accessible by the public, which will effectively reduce copyright owners' damages caused by infringing uploads. For example, when a user tries to upload a newly distributed film on a video platform, without filtering technologies, the uploading would highly likely succeed, and may be watched by many Internet users before it is removed through notice-and-takedown procedure. In these circumstances, irrevocable damage may have been caused to the copyright owner before the infringing upload is taken down, since the public who can watch the film on the video platform may not go to the cinema or buy DVDs. However, if filtering technologies have been adopted, the film cannot be successfully uploaded, and no damage will be caused to the copyright owner. Besides, filtering technologies can also resolve another problem of notice-and-takedown procedure, and that is to prevent the infringing materials from being uploaded again and again. Under notice-and-takedown procedure, the materials that have been removed can be easily uploaded again.[1044] However, in line with UGC Principles and the Self-discipline Declaration, the infringing contents that have been removed can be incorporated into filtering system as reference data, so infringing contents can be effectively prevented from being uploaded again.[1045] As being discussed in Chapter 4, in several cases copyright owners have tried to convince the court that hosting ISPs should adopt filtering technologies, but finally failed, because this claim may conflict with the "no general monitoring obligation" clause.[1046] Nevertheless, through codes of conduct, copyright owners and hosting ISPs agree on a flexible filtering mechanism,[1047] according to which the filtering technologies adopted by hosting ISPs need not to be perfect but state of the art and keep on developing with the efforts of both copyright owners and hosting ISPs. This flexible filtering mechanism not only provides better protection for copyright owners, but also avoid imposing unreasonable burden on hosting ISPs. As noted by

1044 In order to prevent these illegal uploads from being uploaded repeatedly, a French judge had made a "notice-and-staydown" regime, which requests ISPs to take every possible measures to prevent the same content from being uploaded again, but finally, this "notice-and-staydown" regime was rejected by French Supreme Court. See Angelopoulos, 'Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe' (n91), at 265.

1045 Principles for User Generated Content Services (n42), Art. 9. In China, the hosting ISPs who sign the Declaration commonly build the so-called black-content database, and once content has been mentioned in a complaint notice, the content will be input into the black-content database. If the same content is uploaded again, the black-content database can identify it and filter it out.

1046 For instance, in the case of *SABAM v. Netlog*, the plaintiff claimed that the defendant ought to be required to introduce a filtering system for preventing infringing materials from being made available on its platform, but eventually the ECJ dismissed the plaintiff's claim. One of the reasons is that the installation of a filtering system as such would require the defendant to actively monitor all of the information on its platform without time limitation, which would impose a general monitoring obligation on the defendant. See *SABAM v. Netlog* (n311), Para. 43-45, 52.

1047 Anon, 'The Principles for User Generated Content Services: A Middle-Ground Approach to Cyber-Governance' (n960), at 1405.

Prof. Hugenholtz, "norms set by private actors directly concerned are usually geared more precisely to the needs of a specific industry",[1048] so copyright owners and hosting ISPs, as industrial participants, who know exactly what is going on in their industries, can reach an agreement which fits more into the needs of both sides.

When state norms fail to properly define the boundary of hosting ISPs' responsibilities for copyright infringement, through codes of conduct copyright owners and hosting ISPs establish the "best practice" from a business perspective.[1049] Once hosting ISPs comply with the "best practice", they can acquire the copyright owners' promises of not suing them in return. To sum up, under the frame of Codes of Conduct, hosting ISPs avoid assuming unreasonable anti-piracy burden and meanwhile face fewer lawsuits, so Code of Conduct contribute to preserving the freedom to operate of hosting ISPs.

7.1.4.2 Better Legal Certainty

Codes of conduct usually include more detailed norms than state regulation, which makes them easier for hosting ISPs to comply with. For example, NTD Code of Conduct not only includes 7 Articles to instruct the obligations and rights of the parties involved in notice-and-takedown procedures, but also provides explanatory notes which instruct how to interpret these Articles in detail.[1050] Further, codes of conduct also tend to clarify some disputed issues in case law. For instance, when a copyright owner sends a notice to hosting ISPs, it is always a question of whether the URLs of the materials mentioned should be indicated in the notice. In the hearings, copyright owners claim they do not need to offer URLs in notices, but hosting ISPs argue that the URLs are necessary for them to locate the materials, and different courts hold different opinions on this issue.[1051] However, both Code of Conduct and UGC Principles read that the URLs of such materials should be included in notices,[1052] so actually, offering URLs seems not so burdensome as copyright owners claim in the hearings. As industrial participants, what is occurring in the industries is crystallized for them, so they always can reach a more appropriate solution than judges who lack the expertise in relevant industries. In addition, it is also a controversial issue to determine how much time should be allowed for alleged infringing materials to be removed once hosting ISPs receive competent notices. The Self-discipline Declaration in China provides that the infringing materials complained in notices ought to be removed in 24 hours.[1053]

1048 Hugenholtz, 'Codes of Conduct and Copyright Enforcement in Cyberspace' (n55), at 306.

1049 Angelopoulos, C, Filtering the Internet for copyrighted content in Europe (2009) 4 IRIS plus (Supplement to IRIS-Legal Observations of the European Audiovisual Observatory) 2, at 9.

1050 See Notice-and-Take-Down Code of Conduct (n971), and the above discussion about NTD Code of Conduct.

1051 See discussion in previous chapter "notice-and-takedown procedure in the US, the EU and China", Section 5.4.1.

1052 Notice-and-Take-Down Code of Conduct (n971), Art. 4b. Principles for User Generated Content Services (n42), Art. 7.

1053 Self-discipline Declaration, Art. 6.

Codes of conduct can help to achieve certain harmonization in respect of regulating hosting ISPs' copyright responsibilities at international level. The Internet, unlike nations in the physical world, does not have geographic borders, but the application of state regulation has its boundary, and is always connected to a particular nation-state jurisdiction. Based on this inherent conflict between the Internet and state regulation, Professor David Post and David Johnson argued that both the feasibility and legitimacy of state regulation is challenged by the Internet,[1054] and the Internet "cannot be governed, satisfactorily, by any current territorially based sovereign".[1055] Although the effectiveness of state governance on the Internet should not be inappropriately underestimated, state governance does have its own defects when regulating hosting ISPs' copyright responsibilities. Particularly, state governance cannot overcome the restriction set by nations. For instance, the infringing materials uploaded onto hosting platforms can be accessed globally, but the laws and jurisprudence about copyright protection in each nation are different. As can be found from the discussion in previous chapters, even though "safe harbor" provisions have been commonly adopted in the US, EU and China, hosting ISPs' responsibilities for copyright infringement are still diverse in these jurisdictions, which poses barriers for hosting ISPs to operate in these jurisdictions. Codes of conduct can help to overcome the territorial restriction, and set harmonized rules for copyright owner and hosting ISPs in different territories to comply with. Within the leeway left by national laws, UGC Principles are a good example. So far, UGC Principles cover the hosting ISPs and copyright owners based in the US, France and Germany,[1056] and in 2011, even a Chinese video-sharing website called Youku signed the UGC Principles.[1057] These signatory hosting ISPs based in different countries only need to follow the unitary rules set by UGC Principles when dealing with copyright infringement on their platforms.

1054 Johnson and David, 'Post, Law and Borders: The Rise of Law in Cyberspace' (n957), at 1370.

1055 Ibid, at1375.

1056 Principles for User Generated Content Services. 2007. The signatories of UGC Principles include CBS Cooperation, Crackle, Dailymotion (French), Sevenload (Germany), Disney, myspace.com, Veoh, Viacom, etc.

1057 *Youku Joins Broad Coalition in Support of UGC Principles*, PR Newswire(2011), *available at* http://www.prnewswire.com/news-releases/youku-joins-broad-coalition-in-support-of-ugc-principles-117512623.html.

7.1.4.3 Drawbacks of Codes of Conduct

Although Codes of Conduct have advantages in regulating hosting ISPs' copyright responsibilities from the perspective of preserving their freedom to operate, their drawbacks should not be ignored. First, the rules set in self-regulation are not legally enforceable, because self-regulation functions more like an informal understanding among signatories rather than a binding contract.[1058] According to the explanatory statement of the NTD Code of Conduct, "complying with the code is voluntary, and there can be no formal enforcement in the case of non-compliance."[1059] UGC Principles also state that the rules set in Principles should not "be construed as a concession or waiver with respect to any legal or policy position or as creating any legally binding rights or obligations."[1060] In China, the self-regulation documents are titled as self-discipline Treaty or Declaration,[1061] so the self-regulation in China also relies on voluntary enforcement.[1062] Since self-regulation is usually non-binding, the legal certainty is likely to be under threat.[1063] In this regard, hosting ISPs may face a risk of being sued, even though they have already fulfilled the duties prescribed in codes of conduct.

Second, according to codes of conduct, hosting ISPs may need to take the anti-piracy measures that put Internet users' interests in danger, which could bring them legal risks. Regarding the codes of conduct drafted merely by private sectors, they are normally lack of transparency, since the private sectors are not willing to and do not need to reveal the negotiation process, and it is also difficult for the public to know about the creation and existence of self-regulation or even monitor the self-regulation.[1064] Lack of transparency is likely to cause another problem, and that is the Internet users' interests cannot receive proper protection. Further, if only the industrial stakeholders who are directly concerned draft the self-regulation, they tend to defend only their own interests, but leave the Internet users' interests unattended.[1065] The UGC Principles are a typical example. UGC Principles declare that the fair use of hosting service will be accommodated, but are intentionally

1058 See Posting of Sherwin Siy to Policy Blog (Public Knowledge), http://www.publicknowledge.org/node/1230, quoting Anon, 'The Principles for User Generated Content Services: A Middle-Ground Approach to Cyber-Governance' (n960), at 1388.

1059 Notice-and-Take-Down Code of Conduct (n971). See introduction of explanatory statement.

1060 Principles for User Generated Content Services (n42).

1061 See what is discussed in "self-regulation in China" (Section 8.1.3), one document is named as "Self-discipline Treaty on Internet Audio-video Program Services in China", and the other is named as "Self-discipline Declaration on Copyright Protection by Internet Industry in China".

1062 To be mentioned, although Chinese authorities took a leading role in drafting these self-regulation documents, they are not the laws. Certainly, hosting ISPs may face sanctions if they violate the duties set in these documents, but these documents cannot be referred as the basis to decide sanctions against hosting ISPs. Therefore, these self-regulation documents are still non-binding from a legal perspective.

1063 Hugenholtz, 'Codes of Conduct and Copyright Enforcement in Cyberspace' (n55), at 307.

1064 Koop BJ, et al., 'Should Self-regulation be the Starting Point?' in Koops BJ, et al. eds., *Starting Points for ICT Regulation - Deconstructing Prevalent Policy One-liners* (T.M.C. Asser Press. 2006), at 124

1065 Hugenholtz, 'Codes of Conduct and Copyright Enforcement in Cyberspace' (n55), at 307.

"silent on just how such accommodation should take place."[1066] Actually, adoption of filtering technologies seems to naturally contradict the accommodation of fair use. As noted by Michael S. Sawyer, given that fair use is even a big challenge for courts to evaluate, it is almost impossible for any technological solution to reach accurate determinations.[1067] Electronic Frontier Foundation (EFF) also noticed that filtering technologies can hardly accommodate fair use, and then made a proposal to fix the problem.[1068] Further, a filtering mechanism does not provide a proper conduit for users to respond, when the users' uploads are blocked by filters.[1069] Therefore, even if in the case that it is a fair use to incorporate copyrighted materials into uploads, Internet users cannot retrieve their uploads. Moreover, in terms of UGC Principles, hosting ISPs should retain users' uploading data for 60 days,[1070] which may raise privacy concerns. In order to avoid potential liability, hosting ISPs tend to incorporate these norms concerning users into terms of service and users have to accept these boilerplate terms when they make subscriptions.[1071] However, the validity of these terms is subject to the jurisprudence of different jurisdictions. Therefore, hosting ISPs should evaluate whether the anti-piracy measures adopted by them violate the mandatory norms that aim at protecting Internet users' interests. Third, codes of conduct may not be widely representative enough, so their applicability could be limited when regulating hosting ISPs' copyright responsibilities. For instance, the code of conduct like UGC Principles just has a limited number of signatories, and it has been questioned as being not broadly representative enough.[1072] Many big names, such as AOL, Google, Facebook and the four big recording companies, did not sign the UGC Principles.[1073] Without the participation of these high-profile parties, the influence of UGC Principles is largely reduced. Besides, because of their lack of bargaining power, the less influential parties in the industries, including small studios, individual copyright owners, blogs and other small platforms that allow users to post materials, cannot join the negotiations.[1074] Regarding these high-profile companies, they can choose to join the negotiation on

1066 Nathenson IS, 'Civil Procedures for a World of Shared and User-Generated Content' (2010) 48 University of Louisville Law Review 912, at 937.

1067 Sawyer, 'Filters, Fair Use & Feedback: User-Generated Content Principles and the DMCA' (n43), at 366. In part III of this article, Michael made a detailed analysis on why filtering technologies cannot accommodate fair use.

1068 Fair Use Principles for User Generated Video Content, Electronic Frontier Foundation (n43).

1069 Sawyer, 'Filters, Fair Use & Feedback: User-Generated Content Principles and the DMCA' (n43), at 385.

1070 Principles for User Generated Content Services (n42), Art. 10.

1071 Hugenholtz, 'Codes of Conduct and Copyright Enforcement in Cyberspace' (n55), at 309.

1072 Anon, 'The Principles for User Generated Content Services: A Middle-Ground Approach to Cyber-Governance' (n960), at 1387.

1073 Ibid.

1074 Ibid.

codes of conduct and decide whether to join the codes of conduct.[1075] Nevertheless, for these small hosting ISPs, they have almost no chance to join the negotiations that are dominated by several leading players.

7.2 Second Level Agreements

As defined by Yafit Lev-Aretz, a second level agreement is a pre-emptive license acquired by hosting ISPs "in order to ratify the mass usage of copyrighted materials by their users."[1076] Therefore, compared with the codes of conduct which focus on preventing the unauthorized usage of copyrighted materials, second level agreements put the emphasis on legalizing the unauthorized usage of copyrighted materials. The following text will explore the substantial contents of second level agreements, and then examine the advantages and disadvantages of these agreements.

7.2.1 The Substantial Content of Second Level Agreements

Traditionally, if users want to use the materials copyrighted by others, they need to directly negotiate the licenses with copyright owners, and these licenses are first level agreements.[1077] Nevertheless, it is impractical for Internet users to reach the first level agreements as such with copyright owners before they exploit copyrighted materials on hosting platforms, so in fact, a tremendous number of copyright materials are exploited by Internet users without authorization. As discussed in Chapter 3 and 4, the unauthorized exploitation of copyright materials results in lots of lawsuits between copyright owners and hosting ISPs. For the purpose of reducing the lawsuits, hosting ISPs negotiate agreements with copyright owners to deal with the unauthorized exploitation done by Internet users. Although Internet users are not a party to these agreements, these agreements do authorize Internet users to exploit copyrighted materials on a hosting platform, so in this sense, these agreements are named as "second level agreements".[1078] According to the research done by Yafit Lev-Aretz, YouTube is a pioneer in negotiating second level agreements, and thereafter, many other hosting ISPs, including Yahoo!, Myspace, Dailymotion, also signed a series of second level agreement with copyright owners.[1079] In order to examine the substantial contents of second level agreements, a closer look will be done to the agreements reached between YouTube and copyright owners. These agreements usually include the following arrangements: 1) YouTube users are allowed to incorporate the copyrighted works into their videos and upload these videos

1075 For instance, although Google joined the negotiation process of UGC Principles, it did not sign it finally. See Anon, 'The Principles for User Generated Content Services: A Middle-Ground Approach to Cyber-Governance' (n960), at 1387.

1076 Lev-Aretz, 'Second Level Agreements' (n965), at 152.

1077 Ibid, at 152.

1078 Ibid, at 152-153.

1079 Ibid, at 153-154.

onto YouTube; 2) copyright owners set their brand channels on YouTube to provide their professionally-created contents; 3) copyright owners can share the advertising revenue collected not only from videos in their brand channels, but also from the user-generated videos that incorporate the audio and audiovisual works copyrighted by them; 4) copyright owners can request the removal of videos which incorporate the works copyrighted by them; 5) YouTube promised to develop a Content Identification System by which copyright owners can track, monetize or block the contents copyrighted by them. [1080] From the arrangements listed above, one can find that second level agreements basically include two substantial items, one of which is that copyright holders set their brand channels on hosting platforms, and the other content is how to deal with Internet users' uploads which contain copyrighted materials. Regarding these uploads containing copyrighted materials, copyright owners can choose to authorize or block them, and if the uploads are allowed to be uploaded, copyright owners can still choose to monetize or just track them. In order to complete such a complex process, content identification technologies need to be employed.[1081] Therefore, as noted by Yafit Lev-Aretz, second level agreements become standardized after a time, and hosting ISPs who engage in the agreements have commonly adopted content identification technologies.[1082]

Among these content identification technologies, the Content ID system developed by YouTube is most influential because of its dominating role in the video-sharing market. So far, "More than 5,000 partners use Content ID, including major US network broadcasters, movie studios and record labels."[1083] This chapter takes the Content ID system as an example to inspect how content identification technologies work. Content ID system is in essence an automated filtering process, which combines the video fingerprinting technology developed by YouTube and audio fingerprinting technology licensed from Audible Magic.[1084] In order to take advantage of the Content ID system, copyright owners should first fill out a form to claim their right on certain contents,[1085] and deliver the reference files of the content claimed by them to YouTube.[1086] Content

1080 See Warner Music Group and YouTube Announce Landmark Video Distribution and Revenue Partnership (n30); CBS and Youtube Strike Strategic Content And Advertising Partnership (n30); Universal Music Group and Youtube Forge Strategic Partnership (n30); Sony BMG Music Entertainment Signs Content License Agreement with YouTube (n30).

1081 Lev-Aretz, 'Second Level Agreements' (n965), at 152.

1082 Ibid, at 160-161. As pointed out by Yafit Lev-Aretz in this article, after YouTube adopted content identification technologies, the other hosting ISPs, including Myspace, Dailymotion and imeem, also launched content identification technologies. In China, the video-sharing website Youku in China has adopted a similar system called "copyright claim", through which copyright owners can claim their copyright right and join the revenue-sharing program. See *Youku Copyright Cooperation System (优酷版权合作协议)*, Youku, *available at* http://www.youku.com/copyright_apply.html (last visited 12-24-2014).

1083 Statistics-YouTube (2015) (n22).

1084 Steve Chen, *The state of our video ID tools*, Google Offical Blog(2007), *available at* http://googleblog.blogspot.nl/2007/06/state-of-our-video-id-tools.html (last visited 12-24-2014).

1085 *Content Identification Application*, YouTube, *available at* https://www.youtube.com/content_id_signup (last visited 12-24-2014).

1086 How Content ID works (n42).

ID system provides several options for copyright owners when the uploads contain materials matching the reference files delivered by them: mute, block, track or monetize; and copyright owners should make their choices in advance when they deliver the reference files.[1087] Muting means to remove the sound track of videos.[1088] Blocking prevent the whole video from being viewed.[1089] Tracking authorizes copyright owners to get the viewership statistics on the videos containing their copyrighted materials.[1090] Monetizing allows copyright owners to share the ad revenue created by displaying advertisement against the videos that incorporate their claimed contents.[1091]

7.2.2 The Advantages of Second Level Agreements

Within second level agreements, hosting ISPs acquire more legal certainty in operation, and are able to commercially explore the bulk of premium content and provide user-friendlier services. Therefore, second level agreements contribute to enhancing the freedom to operate of hosting ISPs. The following text will explore these advantages of second level agreements in details.

Secondary level agreements are another kind of "best practice" that was initiated by hosting ISPs, and is open for copyright owners to sign up to. Under the frame of second level agreements, hosting ISPs can face fewer lawsuits, because copyright owners receive better protection by cooperating with hosting ISPs in second level agreements. Firstly, second level agreements bring copyright owners new revenue sources, and they can get royalties or share advertising revenue from the hosting ISPs which they have a partnership with.[1092] Secondly, second level agreements can help copyright owners efficiently reduce their enforcement costs, because with the help of content identification technologies "a broader range of potential infringements can be detected at far less cost than is required for manual enforcement."[1093] Without these agreements, copyright owners can merely rely on notice-and-takedown procedures to remove the contents copyrighted by them, which is in fact more costly.[1094] Thirdly, copyright owners are allowed to have multiple choices to deal with the "infringing" uploads according to their needs so that they can maximize their benefits.[1095] For example, if an upload is a full copy of a newly released

1087 Ibid.
1088 Ibid.
1089 Ibid.
1090 Ibid.
1091 Ibid.
1092 In the series of contracts that were signed between YouTube and copyright owners, copyright owners can share the advertising revenue collected not only from videos in their brand channels, but also from the user-generated videos that incorporate the audio and audiovisual works copyrighted by them. See footnote 54. In China, Youku pays royalties to get licenses to offer movies for viewing on its website. See footnote 1082.
1093 Depoorter B and Walker RK, 'Copyright False Positives' (2013), 89 Notre Dame Law Review 319, at 326.
1094 By following notice-and-takedown procedures, copyright owners need to input a certain degree of human resources. For example, NBC Universal had employed three staff whose only responsibility was to daily search for contents owned by NBC Universal but uploaded to platforms without permission, and then send notices to corresponding platforms. See Buckley B, 'SueTube: web 2.0 and copyright infringement' (2007) 31 Columbia Journal of Law & the Arts 235, at 238.
1095 See Content Identification Application, How Content ID works (n42).

movie, the copyright owner can choose to block it so as to ensure its box office revenue. If a copyright owner intends to open up the market for a Television series, it can allow one or two full episodes to be uploaded but with sound track muted. If an upload only contains two minutes of the reference files, the copyright owner may choose to monetize or track it. Fourthly, UGC platforms provide an excellent means for copyright owners to interact with consumers, publicize their contents, and more importantly, copyright owners' contents can receive vast exposure on the platforms.[1096] Even Viacom, who filed a 1 billion dollars lawsuit against YouTube,[1097] recognizes that fans are increasingly willing to "participate with its works through fan sites, fan fiction, mash-ups, and video parodies,"[1098] and hosting ISPs offer the perfect platforms for these fan activities. Overall, secondary level agreements provide several mechanisms which allow copyright owners to maximize their interests. In this regard, signing second level agreements is more attractive to copyright owners than suing hosting ISPs, so second level agreements help to reduce lawsuits faced by hosting ISPs.

Because second level agreements help to reduce lawsuits faced by hosting ISPs, they contribute to increasing the legal certainty in hosting ISPs' operation. As noted by Lev-Aretz, since the boundary of safe harbor is not clear, together with high litigation costs and the potential exposure to damages, ISPs have a strong motivation to build a business partnership with copyright owners so as to protect themselves from lawsuits.[1099] The bankruptcy of Veoh demonstrated how devastating the litigation can be for a hosting ISP. In the case of Veoh, although it won the two copyright lawsuits against it, too high litigation costs still substantially resulted in its bankruptcy.[1100] Besides legal certainty, hosting ISPs also have their income increased by reaching second level agreements with copyright owners. Hosting ISPs' revenue is mainly based on selling ad space on their websites, but in advertisers' eyes, user-generated contents, such as videos of family doing strange things, are usually "incompatible with commercials for cars and other products."[1101] As recognized by Myspace, "although UGC accounts for a majority of video consumed in the United States, the bulk of revenues comes from premium content."[1102] Within Second level agreements, the bulk of premium content is allowed to be available on hosting platforms, and hosting ISPs therefore have more sources to attract advertisers.

1096 Lev-Aretz, 'Second Level Agreements' (n965), at 167. Platforms' advantage on interaction has also been recognized by copyright owners, and Doug Morris, the CEO of Universal Music Group stated, "You Tube is providing a new and exciting opportunity for music lovers around the world to interact with our content", see Universal Music Group and Youtube Forge Strategic Partnership (n30).

1097 Hassanabadi A, 'Viacom v. Youtube: All Eyes Blind–The Limits of the DMCA in a Web 2.0 World' (2011) 26 Berkeley Technology Law Journal 405, at 405.

1098 Nathenson, 'Civil Procedures for a World of Shared and User-Generated Content' (n1060), at 951.

1099 Lev-Aretz, 'Copyright Lawmaking and Public Choice: From Legislative Battles to Private Ordering' (n967), at 252.

1100 Helman L and Parchomovsky G, 'The Best Available Technology Standard' (2011) 111 Columbia Law Review 1194, at 1208.

1101 Barnes B and Stone B, *MGM to Post Full Films on YouTube*, The New York Time(2008), *available at* http://www.nytimes.com/2008/11/10/business/media/10mgm.html?_r=2& (last visited 12-12-2014).

1102 Lev-Aretz, 'Second Level Agreements' (n965), at 160.

Through second level agreements, hosting ISPs are capable of providing services which are friendlier to Internet users. Firstly, a second level agreement to a certain extent functions like a low-cost transaction mechanism over valuable cultural goods.[1103] Taking Content ID as an example, when an upload contains materials matching with the reference files, Content ID "facilitates a 'yes' or 'no' decision by the owner who can then profit from the deal or nix it at a very low cost."[1104] Users can therefore avoid the potential liability for uploading contents copyrighted by others. Secondly, second level agreements can promote the tolerated uses defined by Tim Wu.[1105] According to Tim Wu, "Tolerated use is a term that refers to the contemporary spread of technically infringing, but nonetheless tolerated use of copyrighted works."[1106] Since the enforcing cost may be too high, and infringement may do little harm to or even benefit copyright owners, the copyright owners may choose to tolerate the infringing use.[1107] With the adoption of content identification technologies, copyright owners tend to tolerate more use of their copyrighted contents, because by doing so, they can benefit from tracking or monetizing the videos.[1108] In fact, copyright owners are willing to allow Internet users to exploit their copyright materials. For example, according to the agreement between UMG and YouTube, UMG allows the YouTubers to incorporate its copyrighted music into their user-generated contents.[1109] Therefore, for these creative users who are active on the platforms, there are more raw materials including a wide range of copyright content available for them to create new works.[1110] Overall, by benefiting from second level agreements, Internet users are able to use a wide range of copyright contents without being involved in burdensome negotiation or costly litigation with copyright owners, which will substantially enrich the users' ability of expression.[1111] In this regard, second level agreements allow hosting ISPs to operate in a way which is friendlier to Internet users, and helps hosting ISPs to attract more users.

7.2.3 Disadvantages of Second Level Agreements

Although second level agreements contribute to enhancing the freedom to operate of hosting ISPs, they are highly likely to result in tension between hosting ISPs and their users. In essence, second level agreements are the compromises reached between copyright owners and hosting ISPs, so users' interests tend to be intentionally or

1103 Heald PJ, 'How Copyright Makes Books and Music Disappear (and How Secondary Liability Rules Help Resurrect Old Songs)' (2013) 13 Illinois Program in Law, Behavior and Social Science Paper1, at 32.
1104 Ibid.
1105 Wu T, 'Tolerated Use' (2008) 31 Columbia Journal of Law & Arts 617.
1106 Ibid, at 617.
1107 Ibid, at 619.
1108 Boroughf B, 'The Next Great YouTube: Improving Content ID to Foster Creativity, Cooperation, and Fair Compensation' (2014) 25 Albany Law Journal of Science & Technology 95, at 105.
1109 Universal Music Group and Youtube Forge Strategic Partnership (n30).
1110 Lev-Aretz, 'Second Level Agreements' (n965), at 167-168.
1111 Ibid, at 168.

unintentionally neglected. The following section explores how Internet users' interests are negatively affected in second level agreements, and then assesses the legal risks faced hosting ISPs for these negative effects.

Scholars assert that currently second level agreements offer far more favor to copyright owners than Internet users.[1112] The dispute-settlement mechanism between copyright owners and Internet users is a typical example. Before 2012, after the user filed a dispute against the copyright owners' claim on videos, the Content ID system granted copyright owners rights to make the decision, and the users could not dispute anymore.[1113] This process is very biased in favor of copyright owners, because it in fact deprived users of defending their claims through the notice-and-takedown procedure.[1114] In addition, second level agreements are also vulnerable to change, which put the legal status of UGC in uncertainty. For example, in 2009, UMG could not reach an agreement with YouTube to prolong their cooperation, so UMG terminated the agreement and then signed a new contract with YouTube's competitor – "sevenload".[1115] However, in terms of the pre-existing agreement between UMG and YouTube, UMG had already allowed YouTubers to incorporate its music into their uploads. After the termination of the agreement, how to deal with these uploads containing UMG's music became a complicated issue.[1116]

Besides, second level agreements may have Internet users' uploads wrongly blocked or monetized. First, content identification, as the core of second level agreements, may wrongly block legal contents.[1117] For example, Content ID system has blocked the following videos which are obviously legal: Michelle Obama's Democratic National Convention speech,[1118] NASA's official clips on Mars landing,[1119] and Justin Bieber's music video uploaded by himself.[1120] In addition, second level agreement may result in the abuse of

1112 See generally Simon AR, 'Contracting in the Dark: Casting Light on the Shadows of Second Level Agreements' (2014), 5 William & Mary Business Law Review 305; Boroughf, 'The Next Great YouTube: Improving Content ID to Foster Creativity, Cooperation, and Fair Compensation' (n1102); Lev-Aretz, 'Copyright Lawmaking and Public Choice: From Legislative Battles to Private Ordering' (n967).

1113 Simon AR, 'Contracting in the Dark: Casting Light on the Shadows of Second Level Agreements' (n1106), at 325.

1114 McKay P, *YouTube Copyfraud & Abuse of the Content ID System*, Fair Use Tube(2012), *available at* http://fairusetube.org/youtube-copyfraud (last visited 12-23-2014).

1115 Holger Schmidt, *Die Antwort auf Youtube: Universal-Musikvideos jetzt auf Sevenload*, Frankfurt Allemeine(2009), *available at* http://blogs.faz.net/netzwirtschaft-blog/2009/04/02/die-antwort-auf-youtube-universal-musikvideos-jetzt-bei-sevenload-1014/ (last visited 12-16-2014).

1116 Lev-Aretz, 'Second Level Agreements' (n965), at 172-173.

1117 Boroughf, 'The Next Great YouTube: Improving Content ID to Foster Creativity, Cooperation, and Fair Compensation' (n1102), at 11-12.

1118 Fitzgerald B, *YouTube Pulls Michelle Obama's Democratic National Convention Speech In 'Error'*, The Huffington Post(2012), *available at* http://www.huffingtonpost.com/2012/09/05/youtube-pulls-michelle-obama-speech_n_1857708.html (last visited 12-16-2014).

1119 Higgins P, *Mars Landing Videos, and Other Casualties of the Robot Wars*, Electronic Frontier Foundation(2012), *available at* https://www.eff.org/deeplinks/2012/08/mars-landing-videos-and-other-casualties-robot-wars (last visited 12-16-2014).

1120 Chiang O, *Justin Bieber Swears Off YouTube For Facebook, Unwittingly Steps In Copyright Minefield*, Forbes(2010), *available at* http://www.forbes.com/sites/oliverchiang/2010/11/30/justin-bieber-swears-off-youtube-for-facebook-unwittingly-steps-in-copyright-minefield/ (last visited 12-16-2014).

the copyright claim mechanism. For instance, YouTube requires claimants to have exclusive rights to the materials in videos,[1121] and this means that claimants "cannot claim public domain content, fair use content, or third party content."[1122] However, since the Content ID system makes no front-end copyright ownership verification, the claimants may monetize public domain content.[1123] In some cases, the Content ID system even blocks the contents that copyright owners allow to be exploited by users because of false claims. For example, some game companies had to ask the users to contest the matches and then found out who claimed the content.[1124] Furthermore, like many other filtering technologies discussed above, content identification technologies are not capable of distinguishing between fair use and infringing use,[1125] so fair use content is vulnerable to be monetized or blocked by copyright owners.

The above discussion demonstrates that second level agreements may harm Internet users' interests. Nevertheless, hosting ISPs face little legal risk to do so,[1126] because in order to use hosting services, Internet users need to agree with terms of service which normally grant hosting ISPs the rights to deal with uploads at their discretion and exempt them from removing uploads.[1127] Although there is little risk for hosting ISPs from a legal perspective, they may still need to take better measures to protect Internet users' interests because of the pressure from the public. Taking the above dispute-settlement process adopted by YouTube as an example, since this process incurred lots of criticism in tech blogs and the YouTube help forum, YouTube eventually corrected the undue

1121 *Qualifying for Content ID*, YouTube, *available at* https://support.google.com/youtube/answer/1311402?hl=en (last visited 12-16-2014).

1122 Boroughf, 'The Next Great YouTube: Improving Content ID to Foster Creativity, Cooperation, and Fair Compensation' (n1102), at 9.

1123 Simon, 'Contracting in the Dark: Casting Light on the Shadows of Second Level Agreements' (n1113), at 324.

1124 Crossley R, *Industry fights back as YouTube begins mass cull of game videos*, CVG(2013), *available at* http://www.computerandvideogames.com/442245/industry-fights-back-as-youtube-begins-mass-cull-of-game-videos/ (last visited 12-16-2014).

1125 Boroughf, 'The Next Great YouTube: Improving Content ID to Foster Creativity, Cooperation, and Fair Compensation' (n1102), at 12.

1126 Lev-Aretz, 'Second Level Agreements' (n965), at 177.

1127 For example, according to Art. 7.8 of its Terms of Service – YouTube, once knowing any potential violation of service terms, "YouTube reserve the right (but shall have no obligation) to decide whether the Content complies with the content requirements set out in these terms and may remove such Content and/or terminate a User's access for uploading Content which is in violation of these Terms at any time, without prior notice and at its sole discretion." Further, Art. 13.2 B iii provides that YouTube shall not be liable to users for "the deletion of, corruption of, or failure to store, any Content and other communications data maintained or transmitted by or through your use of the service." See Terms of Service, *available at* https://www.youtube.com/static?template=terms&gl=GB (last visited 08-24-2015). According to Art. 5 of Terms of Use Agreement – Myspace, "Myspace may, in its sole discretion, delete, move, re-format, remove or refuse to post or otherwise make use of Content without notice or any liability to you or any third party in connection with our operation of Content venues in an appropriate manner." See Terms of Use Agreement, *available at* https://myspace.com/pages/terms (last visited 08-24-2015). According to Art. 5.2 of Statement of Rights and Responsibilities, "we can remove any content or information you post on Facebook if we believe that it violates this Statement or our policies." See Statement of Rights and Responsibilities, *available at* https://www.facebook.com/terms.php?ref=pf (last visited 08-24-2015).

process under pressure from the public.[1128] After the reform, when a user files a dispute, Content ID allows copyright owners to have two options: renounce the Content ID claim or initiate the notice-and-takedown procedure.[1129] Further, facing the accusation that Internet users suffer from the false copyright claims under the Content ID system, YouTube announced that it would pay up to 1 million dollars to support its users to defend their own rights.[1130]

Finally, so far, second level agreements can only work as a solution between leading hosting ISPs and high-profile copyright owners, but small copyright owners and small platforms can barely have chance to engage in individual agreement because of their lack of bargaining power.[1131] Further, it is also extremely costly to adopt a complicated content identification system, which means that small hosting ISPs cannot afford to do so. For instance, in order to build a Content ID system, YouTube spent approximately 50,000 man hours on engineering tests and millions of dollars on research and development.[1132] So far, the implementation of second level agreements is limited to specific types of platforms, including audio-and video-sharing platforms, but do not cover image-sharing, blogs and fan fiction websites.[1133] Therefore, many hosting ISPs are unable to engage in second level agreements, and thus cannot enjoy the benefits of such agreements.

7.3 Conclusion:

As has been demonstrated in the previous chapters, although "safe harbor" provisions exempt hosting ISPs from monetary liability under certain circumstances, different courts interpret liability exemption norms in different ways, which poses legal uncertainty for hosting ISPs when conducting business. Further, from the perspective of copyright owners, although they still take the litigation as a weapon against piracy, because of the high cost but limited benefits of the litigation, copyright owners started to turn to reach self-regulation agreements with ISPs.[1134] As noted by Paul Starr, when the public institutions fail to provide a positive public good, the private sector will resort to self-regulation.[1135] In this context, self-regulation becomes more and more prevalent in solving copyright infringement problems on hosting platforms.

1128 Simon, 'Contracting in the Dark: Casting Light on the Shadows of Second Level Agreements' (n1113), at 325.

1129 Higgins P, *YouTube Upgrades Its Automated Copyright Enforcement System*, Electronic Frontier Foundation(2012), *available at* https://www.eff.org/deeplinks/2012/10/youtube-upgrades-its-automated-copyright-enforcement-system (last visited 12-16-2014).

1130 Madore PH, YouTube Will Pay Up To $1 Million in Legal Fees For Qualifying Users, Hacked(2015), *available at* https://hacked.com/youtube-will-pay-1-million-legal-fees-qualifying-users/ (last visited 12-28-2015).

1131 Lev-Aretz, 'Second Level Agreements' (n965), at 171-172.

1132 *Viacom Int'l, Inc. v. YouTube, Inc.*, 253 F.R.D. 256, 260-61 (S.D.N.Y. 2008).

1133 Lev-Aretz, 'Second Level Agreements' (n965), at 111-163.

1134 Bridy A, 'Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement' (2010), 89 Oregon Law Review 81, at 83-84.

1135 Starr P, 'The Meaning of Privatization' (1988) 6 Yale Law & Policy Review 6, at 6.

This Chapter examines two types of self-regulation that have been reached to solve copyright infringement problems on hosting platforms. Generally, codes of conduct focus more on how to reduce copyright infringement on hosting platforms, and second level agreements mainly aim at legalizing the unauthorized exploration of copyrighted materials on hosting platforms. Based on the examination done in this Chapter, it can be concluded that compared to state regulation regimes, these self-regulation agreements are capable of regulating hosting ISPs' copyright responsibilities in a way that enlarges their freedom to operate. First, within self-regulation, hosting ISPs acquire more legal certainty in operation. In the light of self-regulation, copyright owners can receive better protection, which helps hosting ISPs to avoid lawsuits. Further, the norms prescribed in self-regulation tend to be more detailed for hosting ISPs to follow, which contributes to reducing their legal risks in operation. Moreover, the self-regulation agreements like UGC Principles are capable of overcoming the territorial restriction, and harmonizing the rules of hosting ISPs' copyright responsibilities in different jurisdictions. Such harmonization particularly contributes to reducing the legal risks faced by hosting ISPs when operating in different jurisdictions. Second, through self-regulation, hosting ISPs can avoid having an unreasonable burden against copyright infringement, and may even acquire more freedom to exploit materials on their platforms. For instance, second level agreements allow hosting ISPs to commercially exploit the uploads which contain premium materials. Nevertheless, self-regulation also has its weakness in regulating hosting ISPs' copyright responsibilities. First, the applicability of self-regulation is limited. For example, UGC Principles only have limited signatories, and second level agreements so far merely cover limited types of hosting platforms. Particularly, small hosting ISPs, because of lacking bargaining powers, are usually barred from self-regulation. Second, self-regulation, like codes of conduct, is normally not legally enforceable, so hosting ISPs cannot be absolutely secured from liability, even though they've already fulfilled the duties prescribed in self-regulation. Further, within self-regulation, in order to meet the requirement of copyright owners, hosting ISPs need to take some anti-piracy measures which put internet users' interests in danger. From a legal perspective, hosting ISPs face few risks in adopting these measures, because Internet users need to agree with terms of services which usually grant broad rights and liability exemption to hosting ISPs. Nevertheless, hosting ISPs should make sure that the anti-piracy measures adopted by them do not violate the mandatory norms of protecting Internet user's interests. Although self-regulation is not perfect, it is the "best practice" reached between hosting ISPs and copyright owners, and therefore contributes to improving the freedom to operate of hosting ISPs while providing better protection to copyright owners.

List of Publications:

Chapter 3 is an updated version of:

Jie Wang, Not All ISP Conduct is Equally Active or Passive in Different Jurisdictions: Content Liability and Safe Harbour Immunity for Hosting ISPs in Chinese, EU and US Case Law

Published in European Intellectual Property Review (E.I.P.R.), Issue 11, 2015, pp. 732-740.

Parts of Chapter 4 in relation to the US, Germany and China is an updated version of:

Jie Wang, Development of Hosting ISPs' Secondary Liability for Primary Copyright Infringement in China – as Compared to the US and Germany Routes

published in International Review of Intellectual Property and Competition Law (IIC), Vol. 46, 2015, pp. 275-309.

Parts of Chapter 5 in relation to the EU and China are an updated version of:

A research report submitted to the China-EU Law School.

Research project: A Comparative Study on the Secondary Liability of Hosting ISPs

Report title: Notice-and-Takedown Procedures in the EU and China

Part of Chapter 6 in relation to China is an updated version of:

A research report submitted to Google and the University of Washington

Research Project: UW-Google Intermediary Liability Research Project

Report title: Privacy Protection in China

Chapter 7 is an updated version of :

Jie Wang, Self-regulation: a New Way against Copyright Infringement on UGC Websites

A conference paper submitted to and presented at "Intellectual Property Work-in-Progress Colloquium" held in the UW.

Chapter 8

Summary and Conclusion

In the past decade, platforms run by hosting ISPs have gained popularity among Internet users, because they are allowed to access, post, share information and even interact with each other on these platforms. Nevertheless, the popularity of platforms also brings legal risks to hosting ISPs, since many copyrighted materials are uploaded on their platforms without authorization, which may constitute copyright infringement. In the light of rules on indirect copyright infringement, hosting ISPs can be held liable for the copyright infringement committed by their users. In order to ensure hosting ISPs' freedom to operate, "safe harbor" provisions which exempt hosting ISPs from monetary liability under prescribed circumstances have been enacted in the US, EU and China. In this regard, the rules of hosting ISPs' copyright responsibilities have reached certain harmonization in the US, EU and China. However, "safe harbor" provisions in each jurisdiction are not the same and courts tend to interpret "safe harbor" provisions differently because of the jurisprudence in their own jurisdictions. Therefore, despite the common adoption of "safe harbor" provisions, hosting ISPs are still exposed to different copyright responsibilities in the US, EU and China, which increases their legal risks when operating in these jurisdictions. In addition, when deciding hosting ISPs' responsibilities for copyright infringement, courts may impose too much burden on hosting ISPs, which unreasonably restricts their freedom to operate.

Based on the above observation, this book aims at answering a main research question: how to regulate hosting ISPs' responsibilities for copyright infringement while preserving their maximum freedom to operate in the US, EU and China. In order to answer the main research question, this book takes a comparative approach to examine the rules of hosting ISPs' responsibilities for copyright infringement in the US, EU and China. By comparison, this book finds out how to interpret the rules of hosting ISPs' copyright responsibilities so as to maximize their freedom to operate, and concludes whether and how further harmonization can be done regarding regulating hosting ISPs' copyright responsibilities in the US, EU and China. In addition, based on the different copyright responsibilities imposed on hosting ISPs, this book answers the following sub-questions: (i) should hosting ISPs be required to keep purely passive so as to fall under "safe harbor" provisions; (ii) how the courts interpret the factors that are relevant to decide hosting ISPs' copyright liability under "safe harbor" provisions; (iii) whether the liability criteria that developed by the case law are capable of preserving maximum freedom for hosting ISPs to operate; (iv) how notice-and-takedown procedures ought to be interpreted so as to avoid imposing an unreasonable burden on hosting ISPs; (v) whether hosting ISPs should be given more duties to ensure the accuracy of notices; (vi) how hosting ISPs' duties ought to be tailored in identity disclosure mechanisms; (vii) whether self-regulation can better preserve hosting ISPs' freedom to operate.

This chapter summarizes the main findings in the previous chapters and then answers the sub-questions addressed above. It first describes the responsibility rules relevant to copyright enforcement on hosting ISPs' platforms, as addressed in chapter 2 (para. 8.1),

including the liability rules about indirect infringement, and "safe harbor" provisions in the US, EU and China. It then discusses the case law of deciding hosting ISPs' copyright liability in the US, EU and China, and answers the first 3 sub-questions, as concluded in Chapter 3 and 4 (para. 8.2). Next, it explores how the notice-and-takedown procedures and identity disclosure mechanisms are applied in the US, EU and China, and then answers the next 3 sub-questions, as identified in Chapter 5 and 6 (para. 8.3). Subsequently, it explores and evaluates the self-regulation of copyright enforcement on hosting platforms, and then as concluded in Chapter 7, it answers the last sub-question (8.4). Finally, this Chapter lists the concrete conclusions that are reached by this study, and then provides several recommendations to these hosting ISPs who are currently operating or plan to operate in the US, EU and China (8.5).

8.1 Responsibility Rules of Copyright Enforcement on Hosting Platforms

Hosting ISPs' freedom to operate is mainly regulated by the responsibility rules of copyright enforcement on hosting platforms, so Chapter 2 explores these responsibility rules in the US, EU and China so as to draw a full picture of hosting ISPs' responsibilities for copyright infringement on hosting platforms.

Hosting ISPs may be secondarily liable for the copyright infringement committed by their users. Therefore, this chapter firstly explores the secondary liability rules in the copyright field in the US, EU and China. In the EU, there is only limited harmonization in respect of secondary liability in the copyright field, so this chapter looks into the secondary liability rules in several member states, including Germany, France, Italy and the UK. Generally, the secondary liability rules in these jurisdictions are diverse. The common law countries have already developed the specific liability rules about indirect copyright infringement, such as contributory infringement and vicarious liability in the US, authorization infringement and joint tortfeasance in the UK. In civil law countries, such as Germany, France, Italy and China, the courts usually decide the indirect copyright infringement cases by referring to the general liability rules, particularly the duty of care notion, in tort laws.

Besides, this chapter looks into the "safe harbor" provisions which grant hosting ISPs liability privilege in certain conditions. Unlike the secondary liability rules which are varied in the US, EU and China, the liability privilege rules are homogenous per se in these jurisdictions. Based on the comparison, at least three common points can be found. First, hosting ISPs have no general obligation to monitor the materials uploaded on their platforms. Second, in order to benefit from liability exemption, hosting ISPs should not be aware of the infringement in question, or upon knowing the infringement, they should expeditiously remove the infringing materials. Third, hosting ISPs also need to fulfill certain obligations for the purpose of copyright enforcement, such as disclosing suspected users' identities to copyright owners or competent authorities. Regarding

notice-and-takedown procedures, the US and China have codified this procedure in the "safe harbor" provisions, but the E-commerce Directive leaves this procedure for the Member states to develop by themselves. Although the "safe harbor" provisions in the US, EU and China are not the same, they share an important common feature, and that is to exempt hosting ISPs from copyright liability under the prescribed conditions while requiring hosting ISPs to fulfill certain obligations to facilitate copyright enforcement on hosting platforms.

Through the exploration done in Chapter 2, it concludes that in the US, EU and China, the rules of indirect copyright infringement are diverse, but the liability exemption rules – "safe harbor" provisions are homogenous per se. Further, "safe harbor" provisions play an important role in regulating hosting ISPs' responsibilities for copyright infringement, because the "safe harbor" provisions are not only concerned with deciding whether hosting ISPs need to be liable for copyright infringement on their platforms, but also bring in several mechanisms which require hosting ISPs to fulfill certain obligations to facilitate copyright enforcement on their platforms. Based on this observation, the following chapters examine how courts decide hosting ISPs' responsibilities for copyright infringement in the US, EU and China under the roof of "safe harbor" provisions.

8.2 Hosting ISPs' Freedom to Operate and Their Liability for Copyright Infringement

As has been observed in Chapter 2, hosting ISPs may be liable for the copyright infringement on their platforms according to the secondary liability rules in the field of copyright, and meanwhile the "safe harbor" provisions have been adopted to grant hosting ISPs liability privileges under the prescribed conditions. Therefore, Chapter 3 and Chapter 4 examine how the courts in the US, EU and China decide hosting ISPs' copyright liability under the roof of "safe harbor" provisions, and then based on the comparison, these two chapters suggest how the liability rules ought to be interpreted so as to better regulate the hosting ISPs' freedom to operate.

Although hosting ISPs are granted liability privileges by "safe harbor" provisions, the pre-condition is that they are indeed the qualified hosting ISPs defined in the "safe harbor" provisions. Therefore, Chapter 3 examines how to define the qualified hosting ISPs that fall into the "safe harbor" provisions. It is well-known that in the US, EU and China, hosting ISPs are required to remain passive when offering hosting services so as to continue to be under the "safe harbor" provisions. Nevertheless, the courts in the US, EU and China make interpretations about hosting ISPs' "passivity" differently. In China, the courts have held hosting ISPs not passive enough for the following facts: displaying the logos and ads when uploads are viewed, generating the collections of uploaded contents. In the EU, the French, Germany and Italian courts have held hosting ISPs to be publishers or entities similar to publishers based on the following

grounds: for commercially exploiting uploaded contents, for requesting the transfer of rights, for setting different categories for uploading, for allowing subscribers to create their own personal pages, for providing an internal search engine for subscribers to index contents, and for editing the contents uploaded by subscribers. However, nowadays the courts in France, Germany, Italy and China have switched to a standard which is more favorable to hosting ISPs. In China, displaying logos and advertisements cannot be used as reasons for disqualifying hosting ISPs from the "safe harbor" provisions anymore. In France, Italy and Germany, the courts follow the instruction issued by the ECJ in the *Adwords* case, and hold that some hosting ISPs which were once held disqualified for "safe harbor" provisions become qualified now. In the US and UK, the courts have long set a low threshold for hosting ISPs to fall under "safe harbor". In the UK, only when a hosting ISP has edited or controlled the uploaded materials in question, will it be held as a disqualified hosting ISP, and the other factors, such as displaying advertisement, are irrelevant. In the US, a hosting ISP is even allowed to preview the uploaded materials, so long as this preview is done for the purpose of filtering out infringing materials. Further, according to US case law, hosting ISPs are also allowed to employ new technologies to edit the uploaded materials for the purpose of optimizing their services, so long as any editing is done automatically through technical processes.

Based on the exploration of the case decisions in the US, EU and China, Chapter 3 summarizes the factors which have been mentioned which disqualify a defendant as qualified hosting ISP. These factors are: commercially exploiting the uploaded content, editing or categorizing the uploaded content, displaying its logo with uploaded content, requiring rights transfer by "terms and conditions," and uploading some content by itself. After the evaluation of these factors, Chapter 3 concludes that these factors should not function as reasons to exclude hosting ISPs from the "safe harbor," except editing, categorizing, or actively exploiting the uploaded contents. Further, this chapter asserts, it is unreasonable to require hosting ISPs to keep purely passive anymore, and they should be allowed to conduct a degree of management on the uploaded content. In order to draw a proper borderline for permissible management, one first needs to check whether this management will result in a hosting ISP's knowledge or control of uploaded content (the ECJ's opinion), and then check whether this management is conducive to preventing infringements or not (the US approach). This criterion helps to preserve maximum freedom for hosting ISPs to operate, because it not only allows hosting ISPs to employ the new technologies to optimize their services, but also prevents them from optimizing their services for infringing purposes, and even encourages them to actively take measures against copyright infringement on their platforms.

Once a defendant is held as a qualified hosting ISP defined by "safe harbor" provisions, it is still necessary to examine whether the defendant complies with liability privilege conditions set in "safe harbor" provisions. Further, even though the defendant is held as qualifying for liability privilege, it may still face the injunction relief, since "safe harbor"

provisions only exempt it from monetary relief. Chapter 4 discusses how the courts decide hosting ISPs' liability under the roof of "safe harbor" provisions by examining the case decisions in the US, EU and China. Although the courts in different jurisdictions mainly rely on different approaches to decide hosting ISPs' liability, they generally take into account the following factors: (1) hosting ISPs are not obligated to undertake general monitoring responsibility; (2) whether hosting ISPs have specific knowledge of infringement; (3) whether hosting ISPs take reasonable measures against repeat infringement; (4) whether hosting ISPs benefit from infringement; (5) whether hosting ISPs induce infringement, or intend to facilitate infringement.

After examining the case law in the US, EU and China, Chapter 4 concludes that some tendencies of regulating hosting ISPs' secondary liability can be drawn in these jurisdictions. First, because of a "non-general monitoring obligation" clause, in the US and EU, it is not easy to prove hosting ISPs' knowledge of infringement except if they receive competent complaints. In China, hosting ISPs' knowledge of infringement is easier to prove, because the "should know" criterion developed in case law not only covers the US "red flag" test, but also aims at regulating hosting ISPs' business model by requiring them to fulfill a certain duty of care against infringement. Second, "receiving benefits" has become a less important factor for courts to evaluate when deciding hosting ISPs' liability. Normally, courts will not hold hosting ISPs liable only because they make profits in operation. Third, hosting ISPs' intent has become a more prevailing factor when courts conclude liability. Further, courts tend to evaluate hosting ISPs' business models rather than simply checking whether their services are capable of non-infringing use or not. Generally, if a hosting ISP's business model is more likely to result in infringements, it needs to take more effective measures to prevent such infringements. In addition, although a general monitoring responsibility cannot be imposed on hosting ISPs, a specific monitoring responsibility against repeat infringement has been approved by some courts in the EU and China. The specific monitoring responsibility works thus: once infringing content has been identified, the hosting ISP needs to monitor this specific content so as to prevent it from being uploaded again. Besides, compared with the US and EU, China requires hosting ISPs to undertake a higher level of duty of care to prevent hot-play audio-video works and famous works from being uploaded, which can offer better protection for the highly valuable content as such.

Then, Chapter 4 analyzes these factors which mainly affect the hosting ISPs liability in the US, EU and China, and examine how factors ought to be interpreted so as to preserve maximum freedom for hosting ISPs to operate. With respect to hosting ISPs' intent and business model, because the services offered by hosting ISPs are capable of infringing use, any promotion of their services, in a broad sense, can be seen as promoting the infringing use of their services. Therefore, if not restricting the ambit of imputed intent and business models, hosting ISPs will be deterred from adopting new technologies and optimizing their services to attract more subscribers, which will

eventually harm e-commerce. Based on this deduction, Chapter 4 concludes that only when a hosting ISP is proved to have a specific intent to induce copyright infringement, should it be held liable (the US approach). It means the inducement must be actively done through specific acts, such as clear expression or other affirmative steps to foster infringement. By contrast, a general intent to induce, such as the inducement merely deduced from hosting ISPs' business models, should not lead the hosting ISPs to be liable. As for specific monitoring responsibility against repeat infringement, since the boundary between specific monitoring and general monitoring can be blurred, specific monitoring responsibility may impose too much burden on hosting ISPs, which will unreasonably curb hosting ISPs' freedom to conduct business. Further, imposing specific monitoring responsibility on hosting ISPs may also conflict with Internet users' freedom of speech and privacy. Therefore, Chapter 4 suggests that specific monitoring should not be defined as an obligation but rather a positive factor to grant hosting ISPs liability exemption. To be specific, courts should not hold hosting ISPs liable based on the fact that they do not take specific monitoring measures, but if hosting ISPs take specific monitoring measures, courts should hold these efforts as a reason to exempt them from liability. This solution can avoid imposing an unreasonable monitoring burden on hosting ISPs while encouraging them to adopt specific monitoring measures against copyright infringement. Regarding better protection for highly valuable contents, including famous works, hot-playing audio-video works, and content being viewed over a certain number of times, since the boundaries of these highly valuable contents are unclear, hosting ISPs tend to monitor more contents than necessary so as to avoid being held liable. Therefore, without the proper declaration of several terms involved in a higher duty of care, hosting ISPs face high legal uncertainty in operation, and may have to introduce too complicated and costly monitoring systems. In order to avoid unreasonably curbing hosting ISPs' freedom to conduct business, the Chinese courts should either clarify the boundaries of this highly valuable content or stop requiring hosting ISPs to undertake a higher level of duty of care to protect this content.

8.3 Hosting ISPs' Duties to Facilitate Copyright Enforcement

Besides being held liable for copyright infringement under certain circumstances, hosting ISPs also need to fulfill some duties to facilitate copyright enforcement on their platforms. As has been described in Chapter 2, these duties are prescribed in notice-and-takedown procedures and identity disclosure mechanisms. Therefore, Chapters 5 and 6 explore how the notice-and-takedown procedures and identity disclosure mechanisms are applied in the US, EU and China. Then, based on the exploration, these two chapters conclude how the duties of hosting ISPs ought to be regulated in the notice-and-takedown procedures and identity disclosure mechanisms so as to preserve their maximum freedom to operate in these three jurisdictions.

The notice-and-takedown procedure was first codified in the US "safe harbor" provisions. It aims at removing the huge amount of infringing materials on hosting platforms without tedious lawsuits. Ideally, notice-and-takedown procedure works thus: after finding infringing materials on hosting ISPs' platforms, copyright owners send complaining notices to the hosting ISPs, and then the hosting ISPs immediately remove the infringing materials. Because of the efficiency of notice-and-takedown procedure in respect of reducing copyright infringement, China also has codified this procedure into "safe harbor" provisions. In the EU, although the E-commerce Directive does not include a codified notice-and-takedown procedure, it does provide a basis for this procedure, since according to Article 14(1)(b), a notice leading to a hosting ISP's knowledge of infringement will trigger the hosting ISP's obligation to expeditiously take down infringement. Because there is no harmonization at the EU level, the regulation of notice-and-takedown procedures in Member States turns out to be quite fragmented. Some member states have adopted the codified notice-and-takedown procedures, including Finland, Hungary and Lithuania. Some other member states, such as France, Italy and UK, rule on the elements of a competent notice in their national legislation about implementing the E-commerce Directive. There also exist member states which even have not ruled on the elements of a competent notice at legislative level, including Holland and Germany.

248 Generally, the codified notice-and-takedown procedures can achieve better legal certainty, since many issues concerned in notice-and-takedown procedures have been clarified at the legislative level. These issues are: (1) hosting ISPs should set a specific agency to receive notices; (2) the requirement of a competent notice; (3) hosting ISPs should forward the complaining notices to the Internet users whose contents are removed; (4) the elements of counter-notice; (5) hosting ISPs should replace the removed content after receiving counter-notices; (6) who should be liable for any wrong deletion. The clarification of these issues helps the concerned parties, including copyright owners, hosting ISPs and Internet users, know the rights and obligations they have, which can make the notice-and-takedown procedures run more smoothly.

Despite the differences at legislative level, when ruling on notice-and-takedown procedures, the courts in the US, EU and China do have to deal with similar disputable questions. These questions are as follows: how to define a competent notice, how to deal with the defect notices, how to define "expeditiously remove", how to regulate the liability of wrong deletion, and the validity of ex ante notices. The answers to these questions affect the duties of hosting ISPs in notice-and-takedown procedures. Based on examining the case law in the US, EU and China, Chapter 5 concludes how these questions ought to be answered. Regarding how to define a competent notice, the dispute mainly focuses on how exactly the location of alleged infringing materials should be indicated in notices. This chapter argues that it is reasonable to require copyright owners to provide the URLs of infringing materials. Regarding how to deal with defect notices,

the court should approve the validity of a notice which is not fully but substantially in line with the requirement. If a notice is neither fully nor substantially in line with the requirement, but arouses a hosting ISP's strong suspicion of the existence of specific infringing materials, the hosting ISP is obligated to contact the notifier so as to help the notifier perfect the notice. Regarding "expeditiously remove", it is impractical to set a fixed term, and courts should decide in the light of concrete facts in each case, such as the way of sending notices, the accuracy of notices, how hard it is to remove the materials in question and how much material needs to be removed. As for who should be liable for wrong deletion, hosting ISPs ought to be immunized for liability if they conduct the deletion by following notices. Further, copyright owners should be required to send notices in good faith, and otherwise, they should be liable for wrong deletion. Regarding ex ante notices, their validity ought to be dismissed, since if admitting the validity of ex ante notices, hosting ISPs would be imposed a general monitoring obligation which is forbidden by "safe harbor" provisions.

Although the current notice-and-takedown procedures contribute a lot to take down large-scale infringement on the Internet, they also tend to result in wrong deletion. In fact, all three stakeholders, including copyright owners, hosting ISPs and Internet users, contribute to wrong deletion. First, copyright owners tend to send notices without diligent investigation. Second, hosting ISPs are highly likely to remove the materials complained of in the notices so as to reduce the risks of being sued by copyright owners. Third, Internet users normally do not send counter-notices even when their materials are wrongly taken down. After examining the measures that have been adopted to reduce wrong deletion, this chapter asserts, in order to substantially curb wrong deletion, copyright owners rather than hosting ISPs should be given more duties to ensure the accuracy of notices, such as taking fair use into account when sending notices. If requiring hosting ISPs to be responsible for reducing wrong deletion, they need to evaluate notices like private judges, but this goes beyond their capacity and therefore imposes unreasonable burden on their freedom to operate.

Overall, in notice-and-takedown procedures, copyright owners ought to shoulder the responsibility of seeking and identifying infringing materials, and the duty of hosting ISPs is to help copyright owners protect their rights, such as expeditiously removing the suspected infringing materials after receiving notices. Further, hosting ISPs also function as a communication conduit between copyright owners and Internet users, such as forwarding notices and counter notices. Regarding wrong deletion, more duties should be imposed upon copyright owners rather than on hosting ISPs in order to reduce it. Distributing duties between copyright owners and hosting ISPs in this way can avoid imposing an unreasonable burden on hosting ISPs in notice-and-takedown procedures, and thus helps to preserve maximum freedom for hosting ISPs to operate.

In order to help copyright owners identify anonymous infringers on the Internet, hosting ISPs are obligated to disclose the infringers' identities under certain circumstances.

From the perspective of avoiding the conflicts with copyright owners, hosting ISPs are more willing to disclose alleged infringers identity information to them, but because of privacy concerns, the identity disclosure should be conducted in a due process. Chapter 6 examines the identity disclosure mechanisms in the US, EU and China. In the US, DMCA 512 (h) provides a green channel for copyright owners to request internet users' identities, according to which, a copyright owner or its agents can request the clerk of any US District Court to issue a subpoena for disclosing the identity of an alleged infringer. Besides the "green channel", copyright owners can also file John Doe subpoenas to request hosting ISPs to disclose the suspected infringers' identities. In the EU, the relevant directives and ECJ decisions also allow the suspected infringers' identities to be disclosed in copyright cases. The identity disclosure mechanisms have also been established in the Member States, such as "Norwich Pharmacal orders" in the UK, Section 101 (1) of the Germany Copyright Act and Article 156bis of Italian Copyright Law. In the US and EU, hosting ISPs are only subject to the disclosing orders of competent authorities, and if copyright owners want to acquire the identity information of suspected infringers, they need to apply for court orders. By contrast, in China, no specific procedural requirement is imposed on disclosing Internet users' identities in civil proceedings, and upon the request of copyright owners, hosting ISPs can even disclose Internet users' identities without judicial review.

250 Based on the exploration of identity disclosure mechanisms in the US, EU and China, it can be found that hosting ISPs' duties are mainly based on the answers to these two questions: (1) under what circumstances is a hosting ISP obligated to conduct disclosure; (2) to what extent should a hosting ISP disclose a suspected infringer's identity. Because of privacy concerns, hosting ISPs should be forbidden to voluntarily disclose suspected infringers' identities to copyright owners without orders from courts or competent authorities. Regarding the second question, hosting ISPs are only obligated to disclose the identity information retained by them. Nevertheless, hosting ISPs normally do not retain enough personal data to have suspected infringers successfully identified, so the effectiveness of identity disclosure is in question. China has solved this problem by adopting a "real-name registration" policy. In the light of this policy, hosting ISPs should require Internet users to submit their real identity information when registering for their services. Because of concerns on freedom of speech, a similar policy can hardly be transposed into the US and EU. In addition, it is also inappropriate to require hosting ISPs to retain Internet users' online communication data because of privacy concerns, although imposing such an obligation on hosting ISPs helps to solve the effectiveness problem of identity disclosure mechanisms.

Overall, in identity disclosure mechanisms, hosting ISPs assume a passive obligation, and that is to disclose the identity information of alleged infringers to the extent such information is available to them, upon receiving orders from competent third parties. Further, they are not responsible for the failure of identifying suspected infringers once

they disclose the identity information retained by them. In addition, hosting ISPs should be forbidden to disclose their users' identity information to copyright owners without court orders. These duties require a little effort to fulfill, and do not unreasonably restrict hosting ISPs' freedom to operate.

8.4 Duties under Self-regulation

Besides state regulation discussed above, self-regulation gains popularity between copyright owners and hosting ISPs to solve the copyright disputes on hosting platforms. In the light of self-regulation, copyright owners and hosting ISPs cooperate with each other so as to reduce copyright infringement on hosting platforms. Generally, self-regulation can be divided into two types - codes of conduct and second level agreements. Regarding codes of conduct, they are the result of the cooperation and compromise between multiple copyright owners and hosting ISPs, such as UGC Principles, but government may be also engaged with a variety of gravities, such as NT Code of Conduct in the Netherlands and Self-discipline Codes in China. Generally, copyright owners and hosting ISPs, as industrial participants, who know exactly what is going on in their own industries, can reach an agreement which better fits the needs of both sides. Therefore, codes of conduct can better preserve hosting ISPs' freedom to operate when solving copyright disputes between hosting ISPs and copyright owners on hosting platforms. First, codes of conduct avoid imposing unreasonable burdens on hosting ISPs, since any duty which is too burdensome for them would not be agreed by hosting ISPs. Second, codes of conduct contribute to increasing the legal certainty faced by hosting ISPs in operation. In the light of codes of conduct, hosting ISPs promise to undertake more responsibilities against copyright infringement, and once hosting ISPs fulfill these responsibilities, copyright owners usually will not sue them. Further, the norms prescribed in codes of conduct tend to be more detailed than statutory rules, which make them easier for hosting ISPs to comply with.[1136] Moreover, codes of conduct like UGC Principles can overcome the restriction of sovereignty, and internationally harmonize the rules of regulating hosting ISPs' responsibilities for copyright infringement. Nevertheless, codes of conduct also have drawbacks. First, codes of conduct are non-binding, which means they are not enforceable from a legal perspective. Further, codes of conduct also have limited applicability. Regarding the codes of conduct achieved solely between private entities, such as UGC Principles, it is almost impossible for small hosting ISPs to join the negotiation because of lacking bargaining powers. Moreover,

1136 Taking notice-and-takedown procedure as an example, the NT Code of Conduct and UGC Principle clearly request copyright owners to submit the URLs of infringing materials in notices, and Self-discipline Declaration requires hosting ISPs to remove the designated materials in 24 hours upon receiving notices. See Section 7.1.3.2 and 7.1.2. In contrast, the codified notice-and-takedown procedures in the US and China do not address whether the URLs of infringing materials should be included in notices and what constitutes "immediately remove". See Section 5.4.1 and 5.4.2.

within codes of conduct, hosting ISPs may need to take some anti-piracy measures which put Internet users' interests in danger.

Besides codes of conduct, copyright owners and hosting ISPs have also reached a wide range of second level agreements. Unlike the codes of conduct which focus on preventing the unauthorized usage of copyrighted materials, second level agreements emphasize more the legalizing of the unauthorized usage of copyrighted materials. As time goes by, second level agreements have become standardized. In the light of second level agreements, hosting ISPs are commonly required to adopt content identification technologies, which allow copyright owners to track, block and monetize Internet users' uploads which contain their copyrighted materials. Content identification technologies to a certain degree function like a low-cost transaction mechanism over valuable cultural goods, because they allow copyright owners to make a "yes" or "no" decision, when an upload contains materials matching the reference files.

Second level agreements have many advantages in preserving hosting ISPs' freedom to operate. First, within second level agreements, copyright owners receive better protection, which helps to reduce the lawsuits faced by hosting ISPs. By signing second level agreements, copyright owners can benefit from receiving new revenue, reducing enforcement costs and better interacting with fans. Further, they can maximize their benefits, because content identification technologies allow them to have multiple choices to deal with the uploads that contain their copyrighted materials. Second, by reaching second level agreements with copyright owners, hosting ISPs have more freedom to commercially exploit the materials uploaded by their users, and attract more advertisers because more professionally-created contents are available on their platforms. Further, individual agreements can even create positive externalities on Internet users. Within second level agreements, Internet users are able to use a wide range of copyright contents without being involved in burdensome negotiation or costly litigation with copyright owners, which will substantially enrich the users' ability of expression. Nevertheless, second level agreements are in essence the compromises reached between copyright owners and hosting ISPs, so users' interests tend to be intentionally or unintentionally neglected. Besides, the applicability of second level agreements is also limited. So far, second level agreements are mainly applied to audio- and video-sharing platforms, but picture-sharing, blogs and fan fiction websites are outside second level agreements. Further, small hosting ISPs are also barred from second level agreements because of their limited bargaining power and costly content identification systems.

Overall, compared with state regulation regimes, self-regulation can better preserve freedom for hosting ISPs to operate. Within a self-regulation regime, hosting ISPs face more legal certainty in operation. Further, self-regulation can avoid imposing unreasonable burdens on hosting ISPs, and even entitle more freedom to hosting ISPs to commercially exploit the content on their platforms. Nevertheless, the applicability of self-regulation is limited, and particularly, small hosting ISPs can hardly join the self-

regulation agreements controlled by several dominating market players. Further, self-regulation is generally the "best practice" reached between copyright owners and hosting ISPs, so Internet users' interests tend to be paid less attention. Some self-regulation agreements require hosting ISPs to take the anti-piracy measures which put Internet users' interests in danger. From the legal perspective, hosting ISPs can usually avoid being held liable for adopting these measures, because Internet users need to agree with the "terms of services" before using the services, and the "terms of services" grant wide rights and liability exemptions to hosting ISPs. Nevertheless, the measures taken by hosting ISPs should avoid violating the mandatory norms which aim at protecting Internet users' interests.

8.5 Conclusions and Recommendations

The services provided by hosting ISPs facilitate copyright infringement on the Internet, and for the purpose of protecting copyright, certain copyright responsibilities have been imposed on hosting ISPs, which restrains their freedom to operate. This book first explores the copyright responsibilities imposed on hosting ISPs by state regulation, including secondary liability and the duties of facilitating copyright enforcement as prescribed in notice-and-takedown procedures and identity disclosure mechanisms. Then, it suggests how these copyright responsibilities ought to be tailored so as to better regulate hosting ISPs' freedom to operate. Moreover, it explores how the freedom to operate of hosting ISPs is regulated under a self-regulation regime, and points out that self-regulation does have some advantages over state regulation in respect of regulating hosting ISPs' freedom to operate.

Based on the study in this book, the following concrete conclusions can be drawn:

(i) It is no longer proper to require hosting ISPs to keep purely passive, and they should be allowed to conduct certain management of uploaded content. Nevertheless, such management cannot result in hosting ISPs' knowledge or control of the uploaded content. In addition, the management that helps the prevention of infringement should be also allowed. (Section 3.5)

(ii) Hosting ISPs do not need to undertake a general obligation to monitor the content uploaded by Internet users. (Section 4.1) Hosting ISPs' knowledge of infringement cannot be easily concluded without notices from copyright owners, except in China. (Section 4.2) "Receiving benefits" has become a less important factor for courts to evaluate when deciding hosting ISPs' liability. (Section 4.4) Hosting ISPs' intent and business model become a prevailing factor for courts to evaluate when deciding liability. (Section 4.5) Specific monitoring obligations against repeated infringement have been developed by some courts in the EU and China. (Section 4.3) In China, hosting ISPs are

required to undertake a higher level of duty of care to protect highly valuable content. (Section 4.6)

(iii) These liability criteria that developed by case law, including the intent and business model of hosting ISPs, specific monitoring obligations against repeated infringement, and higher level of duty of care to protect highly valuable content, need to be refined so as to avoid imposing an unreasonable burden on hosting ISPs. (Section 4.7 and 4.8)

(iv) A competent notice should be required to include the URLs of infringing materials. It is impractical to set a fixed term to regulate what constitutes "expeditiously removing", and it ought to be decided by courts based on the concrete facts in each case. The notices which substantially comply with the requirement should be deemed as valid. Hosting ISPs need to help copyright owners to perfect their notices, once the defect notices arouse their strong suspicion of existing infringing materials. Hosting ISPs do not need to be liable for wrong deletion, if they faithfully conduct deletion by following the notices. The validity of ex ante notices ought to be denied. (Section 5.4)

(v) The current notice-and-takedown procedures are easily abused and result in wrong deletion. In order to substantially reduce wrong deletion under notice-and-takedown procedures, copyright owners rather than hosting ISPs should be imposed more duties to ensure the accuracy of notices. (Section 5.5)

(vi) Hosting ISPs are obligated to disclose suspected infringers' identity information only after receiving orders from competent authorities, and they should be forbidden to conduct such disclosure to copyright owners without orders from competent authorities. Further, hosting ISPs are only obligated to disclose suspected infringers' identity information retained by them, and should not be held responsible for the failure of identifying suspected infringers once they have disclosed the identity information retained by them. (Section 6.4 and 6.5)

(vii) Although Self-regulation is not perfect in regulating hosting ISPs' responsibilities for copyright infringement, it helps to preserve better the freedom to operate of hosting ISPs. (Section 7.1.4, 7.2.2 and 7.2.3)

Besides the conclusions listed above, this book provides some recommendations for these hosting ISPs who are now operating or have a plan to operate in the US, EU and China.

(i) It is better for hosting ISPs to adopt technical filtering measures against infringing materials, especially the infringing materials which are repeatedly uploaded. In the EU and China, case law imposes specific monitoring obligations on hosting ISPs, and requires them to take reasonable measures to prevent infringing materials from being repeatedly uploaded. In the US, although case law does not explicitly require hosting ISPs to assume such specific monitoring obligations, the US courts do see the efforts of adopting technical filtering measures as evidence to prove hosting ISPs' fulfilling of their anti-piracy duties. (Section 4.3)

(ii) For hosting ISPs who are operating in China, it is better for them to monitor the following content: (1) the materials that are uploaded to the channel "movies and television series"; (2) famous works and hot-playing audio-video works; (3) the uploads that have been viewed over a certain number of times. In China, the case law requires hosting ISPs to assume the obligations of monitoring these highly valuable contents. (Section 4.6)

(iii) From the perspective of avoiding liability, once having received notices from copyright owners, it is better for hosting ISPs to expeditiously remove the suspected infringing materials that are complained about in the notices. If the materials indicated in notices are proved to be infringing, but hosting ISPs did not expeditiously remove them upon receiving notices, hosting ISPs would be held liable. If the materials indicated in the notices are proved to be non-infringing, it is commonly held in the US, EU and China that copyright owners rather than hosting ISPs ought to be responsible for wrong deletion. Therefore, even if hosting ISPs conduct wrong deletion by following notices, they would not be held liable. (Section 5.4.4)

(iv) Hosting ISPs must refrain from promoting the infringing use of their services in operation. In the US, EU and China, when courts decide hosting ISPs' liability, they evaluate whether hosting ISPs encourage or induce their users to commit copyright infringement. (Section 4.5)

(v) Hosting ISPs should be actively engaged in self-regulation, and then establish their freedom to operate by negotiating with copyright owners. Self-regulation is the "best practice" reached between hosting ISPs and copyright owners. Within self-regulation, hosting ISPs can face fewer legal risks and acquire more legal certainty in operation. (Section 7.3)

8.6 Closing Remark

This book discusses hosting ISPs' responsibilities for copyright infringement in the US, EU and China, and particularly examines how the current responsibility rules ought to be interpreted or revised so as to preserve maximum freedom for hosting ISPs to operate in these jurisdictions. Besides examining the state regulation, this book also assesses self-regulation norms reached between copyright owners and hosting ISPs, and concludes that self-regulation can better preserve hosting ISPs' freedom to operate. The legislative history of "safe harbor" provisions in the US, EU and China suggests that it is necessary to strike a balance between copyright protection, hosting ISPs' freedom to operate and Internet users' interests.[1137] Nevertheless, this research mainly focuses on how to interpret the "safe harbor" provisions from the perspective of preserving the freedom to operate of hosting ISPs. Therefore, although this research takes into account copyright protection and Internet users' interests, when regulating hosting ISPs' copyright responsibilities, it does not make sure that the result of this research fits in with the delicate balance that is expected by the policy makers in each jurisdiction. Further, this research recognizes that it helps to preserve maximum freedom for hosting ISPs to operate in the US, EU and China, if harmonization can be achieved in the rules of regulating hosting ISPs' responsibilities for copyright infringement. However, full harmonization at both legislative and judicial levels is too complicated a project for this research to manage, so this research mainly focuses on further harmonization in interpreting "safe harbor" provisions at the judicial level.

Based on the research done in Chapter 7, it can be found that self-regulation has certain advantages over state regulation in regulating hosting ISPs' responsibilities for copyright infringement. Particularly, self-regulation can better reconcile the conflicts between copyright protection and hosting ISPs' freedom to operate. Therefore, it would be a wise choice for state regulation to take advantage of self-regulation so as to regulate hosting ISPs' responsibilities for copyright infringement. In fact, some efforts have been made to integrate self-regulation into state regulation.[1138]

1137 As stated in a legislative document of the E-commerce Directive, the liability rules of intermediaries should strike a delicate balance between the different interests concerned and promote cooperation between different parties so as to reduce the infringement on the Internet. See IP/98/999 'Electronic Commerce: Commission Proposes Legal Framework' (n14). The legislative document of DMCA also notes that it is necessary to balance the interests of copyright owners, online service providers and information users in a proper way so as to foster the development of e-commerce. See H.R. REP. 105-551(II), (n16) at 21. In China, Internet Regulation also aims at reconciling the interests of copyright owners, ISPs and Internet users. See Legislative Affair Office Answered Reporters' Questions on "Regulation on the Protection of the Right to Internet Dissemination of Information" (法制办就《信息网络传播权保护条例》答记者问) (n33).

1138As being provided in the Australia Copyright Act, Sec. 36 (1A), when deciding whether a person authorizes the copyright infringement concerned, the court should take into account "whether the person complied with any relevant industry codes of practice" to prevent or avoid the infringement. In Hong Kong, according to the Sec. 88B(3) of Copyright (Amendment) Bill 2014, when deciding whether an ISP takes reasonable measures to limit or stop copyright infringement, the court should take account of whether the ISP complies with all the provisions in the Code of Practices. Further, In China, although it is not a statutory rule for courts to refer to self-regulation norms when deciding cases, many courts still consider whether hosting ISPs have adopted the measures as prescribed in self-regulation to prevent infringement from occurring, when they hear the cases about hosting ISPs' liability.

Nevertheless, how to integrate self-regulation into state regulation is still an ongoing issue, which needs further study. Moreover, self-regulation also needs state regulation to overcome its disadvantages, such as a lack of binding power, not widely representative, trampling on internet users' interests.[1139] Nevertheless, how and in what way should state regulation step into self-regulation is still in question. Therefore, it is meaningful to study how to regulate hosting ISPs' responsibilities for copyright infringement by the integration of self-regulation and state regulation. Nevertheless, how to accomplish such integration is a far-reaching question,[1140] which goes beyond the discussion in this book, and the author leaves it for study in the future.

1139 If self-regulation is "not completely dependent on statutory legal regulators, informal institutions can play an important role in shaping and ordering online conduct"; and ideally, besides taking advantage of private actors' flexibility and their expertise in internet technologies, self-regulation also needs the government's involvement to ensure full representation in drafting process. See Anon, 'The Principles for User Generated Content Services: A Middle-Ground Approach to Cyber-Governance' (n960), at 1405-1406. As observed by Netanel, it is almost impossible for self-regulation, which aims at solving the disputes among internal parties, to care about reducing harmful externalities to outsiders, so such self-regulation should work under the oversight of government. See Netanel NW, 'Cyberspace Self-governance: A Skeptical View from Liberal Democratic Theory' (2000) 88 California Law Review 395, at 476. Easterbrook, as an advocate of self-regulation in cyberspace, also acknowledges the importance of state regulation, and points out that formal regulations need to set norms that contribute to bargaining between stakeholders, including making rules clearer, creating property rights and creating bargaining institutions. See Easterbrook, 'Cyberspace and the Law of the Horse' (1996) 1 University of Chicago Legal Forum 207 (n958).

1140 Since the 1990s, how to regulate activities on the Internet through integrating self-regulation with state regulation has been an ongoing issue that arouses lots of discussion. So far, from a theoretical perspective, there are mainly three diverse approaches to integration, which are the co-regulation approach, the hybrid arrangements approach and the substitution approach, and academics and practitioners have delivered strong arguments for each of these approaches. See Bonnici, J. P. M., *Self-regulation in cyberspace* (Cambridge University Press. 2008), at 9-22.

Bibliography

Articles and books:

- Angelopoulos C, 'Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe' (2013) 3 Intellectual Property Quarterly 253 n107
- Anon, 'The Principles for User Generated Content Services: A Middle-Ground Approach to Cyber-Governance' (2008) 121 Harvard Law Review 1387
- Baraliuc I, Depreeuw S, and Gutwirth S, 'Copyright enforcement in the digital age: a post-ACTA view on the balancing of fundamental rights' (2013) 21 International Journal of Law and Information Technology 92
- Barazza S, 'Secondary liability for IP infringement: converging patterns and approaches in comparative case law' (2012) 7 Journal of Intellectual Property Law & Practice 879
- Batholomew M and Tehranian J, 'Secret Life of Legal Doctrine: The Divergent Evolution of Secondary Liability in Trademark and Copyright Law' (2006) 21 Berkeley Technology Law Journal 1363
- Bayer J, Liability of Internet Service Providers for Third Party Content (2008) 1 Victoria U. Wellington Working Paper Ser. 1
- Bellan A, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in Italy' in Heath C and Sanders AK eds., *Intellectual Property Liability of Consumers, Facilitators, and Intermediaries* (Kluwer Law International 2012)
- Bonnici, J. P. M., *Self-regulation in cyberspace* (Cambridge University Press. 2008)
- Bently L and Sherman B, *Intellectual property law* (Oxford University Press. 2008)
- Blakeney S, 'The Data Retention Directive: combating terrorism or invading privacy?' (2007) 13 Computer and Telecommunications Law Review 153
- Bonadio E and Santo M, 'Court of Milan holds video sharing platforms liable for copyright infringement' (2012) 7 Journal of Intellectual Property Law & Practice 14
- Boroughf B, 'The Next Great YouTube: Improving Content ID to Foster Creativity, Cooperation, and Fair Compensation' (2014) 25 Albany Law Journal of Science & Technology 95
- Bretan J, 'Harboring Doubts about the Efficacy of 512 Immunity under the DMCA' (2003) 18 Berkeley Technology Law Journal 43
- Bridy A, 'Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement' (2010), 89 Oregon Law Review 81
- Buckley B, 'SueTube: web 2.0 and copyright infringement' (2007) 31 Columbia Journal of Law & the Arts 235
- Carmichael J, 'In Support of the White Paper: Why Online Service Providers Should Not Receive Immunity from Traditional Notions of Vicarious and

Contributory Liability for Copyright Infringement' (1995) 16 Loyola of Los Angeles Entertainment Law Review 759
- Cobia J, 'The Digital Millennium Copyright Act Takedown Notice Procedure: Misuses, Abuses, and Shortcomings of the Process' (2008), 10 Minnesota Journal of Law, Science & Technology 387
- Cohen JE, 'Lochner in Cyberspace: The New Economic Orthodoxy of" Rights Management' (1998) 97 Michigan Law Review 462
- Cohen JE, 'Overcoming Property: Does Copyright Trump Privacy?' (2002) 2002 Journal of Law, Technology & Policy 375
- Cohen JE, Loren LP, Okediji RL, O'Rourke MA, *Copyright in A Global Information Economy*, (Aspen Publisher 2010 (3rd))
- Coraggio G, 'Google's victory might be a short success' (2012) 23 Entertainment Law Review 139
- Cunard J and Wells A, 'The Evolving Standard of Copyright Liability Online' (1997) 497 PLI/Pat 365
- de Azevedo Cunha, M. V., Marin, L., & Sartor, G., 'Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web' (2012) 2 International Data Privacy Law 50
- Easterbrook FH, 'Cyberspace and the Law of the Horse' (1996) 1 University of Chicago Legal Forum 207
- Edwards L, 'Should ISPs be Compelled to Become Copyright Cops? File-Sharing, the Music Industry and Enforcement Online' (2009) 19 Journal of the Society for Computers and Law 29
- Feiler L, '*The legality of the data retention directive in light of the fundamental rights to privacy and data protection'* (2010) 1 European Journal of Law and Technology 3
- Fitzner J, Von Digital-Rights-Management zu Content Identification: *Neue Ansätze zum Schutz Urheberrechtlich Geschützter Multimediawerke im Internet: Eine Technische, ökonomische und Rechtliche Analyse* (Nomos. 2011)
- Friedman B, 'From Deontology to Dialogue: The Cultural Consequences of Copyright' (1994) 13 Cardozo Arts & Entertainment Law Journal 157
- Gendreau Y, 'Authorization revisited' (2000) 48 Journal of the Copyright Society of the U.S.A. 341
- *Germany: "Rapidshare III" - Telemedia Act secs.7(2), 10* (2014), 45 International Review of Intellectual Property and Competition Law 716
- Gibbon LJ, 'No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace' (1996) 6 Cornell Journal of Law and Public Policy 475
- Ginsburg JC, 'Tale of Two Copyrights: Literary Property in Revolutionary France and America' (1989) 64 Tulane Law Review 991

- Ginsburg JC, 'Putting Cars on the" Information Superhighway": Authors, Exploiters, and Copyright in Cyberspace' (1995) 95 Columbia Law Review 1466
- Ginsburg JC, 'Copyright and control over new technologies of dissemination' (2001) 101 Columbia Law Review 1613
- Wu HD(吴汉东), 'Study of Internet Service Providers' Liability for Copyright Infringement (论网络服务提供者的著作权侵权责任)' (2011) 2 China Legal Science (中国法学) 38, at 38-47.
- Hardy IT, 'The Proper Legal Regime for Cyberspace' (1993) 55 University of Pittsburgh Law Review 993.
- Heald PJ, 'How Copyright Makes Books and Music Disappear (and How Secondary Liability Rules Help Resurrect Old Songs)' (2013) 13 Illinois Program in Law, Behavior and Social Science Paper1
- Heath C and Liu KC, *Copyright Law and the Information Society in Asia* (Bloomsbury Publishing 2006)
- Hegel, GW and Knox TM, *Hegel's philosophy of right* (Oxford University Press. 1967)
- Heins M and Beckles T, Will Fair Use Survive? Free Expression in the Age of Copyright Control (Brennan Center For Justice 2005)
- Hocking R 'Secondary liability in copyright infringement: still no Newz?' (2012) 23 Entertainment Law Review 83
- Holznagel D, 'Melde- und Abhilfeverfahren zur Beanstandung rechtswidrig gehosteter Inhalte nach europäischem und deutschem Recht im Vergleich zu gesetzlich geregelten notice and take-down-Verfahren' (2014) GRUR Int. 105
- Högberg SK, 'The Search for Intent-Based Doctrines of Secondary Liability in Copyright Law' (2006) 106 Columbia Law Review 909
- Hugenholtz PB, 'Codes of Conduct and Copyright Enforcement in Cyberspace' *in* Stamatoudi IA (eds), *Copyright Enforcement and the Internet* (Kluwer Law International, 2010)
- Hughes J, 'Philosophy of Intellectual Property' (1988) 77 Goergetown Law Journal 287
- Kaiser AB, 'German data retention provisions unconstitutional in their present form; decision of 2 March 2010, NJW 2010, p.833' (2011) 6 European Constitutional Law Review 503
- Jan Bernd Nordemann, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: The Position in Germany' in Heath C and Sanders AK eds., *Intellectual Property Liability of Consumers, Facilitators, and Intermediaries* (Kluwer Law International 2012)
- Johnson DR and David G, 'Post, Law and Borders: The Rise of Law in Cyberspace' (1996) 48 Stanford Law Review 1367.
- Koop BJ, et al., 'Should Self-regulation be the Starting Point?' in Koops BJ, et al. eds., *Starting Points for ICT Regulation - Deconstructing Prevalent Policy One-liners*

(T.M.C. Asser Press. 2006)
- Köhler C and Burmeister K, 'Copyright liability on the Internet today in Europe (Germany, France, Italy and the E.U.)' (1999) 21 European Intellectual Property Review 485
- Kuner C, 'Data protection and rights protection on the internet: The Promusicae judgment of the European court of justice' (2008) 30 European Intellectual Property Review 199
- Kuner C, et al., Study on online copyright enforcement and data protection in selected Member States (2009), DG Internal Market and Service of European Commission
- Leistner M, 'Structural aspects of secondary (provider) liability in Europe' (2014) 9 Journal of Intellectual Property Law & Practice 75
- Lemley MA. and Reese RA, 'Reducing digital copyright infringement without restricting innovation' (2004) 56 Stanford Law Review 1345
- Lemley MA, 'Property, intellectual property, and free riding' (2004) 83 Texas Law Review 1031. Mossoff A, 'Is copyright property' (2005) 42 San Diego Law Review 29
- Lemley MA, 'Rationalizing Internet Safe Harbors' (2007) 6 Journal of Telecommunications and High Technology Law 101
- Lichtman D and Landes W, 'Indirect liability for copyright infringement: an economic perspective' (2003), 16 Harvard Journal of Law & Technology 395
- Liu JR, 'Why is Betamax an Anachronism in the Digital Age?–Erosion of the Sony Doctrine and Indirect Copyright Liability of Internet Technologies' (2005) 7 Vanderbilt Journal of Entertainment and Technology Law 243
- Liu JR (刘家瑞), 'ISP Safe Harbours in China (论我国网络服务商的避风港规则--兼评"十一大唱片公司诉雅虎案")' (2009), 19 Intellectual Property (知识产权) 13
- Llewelyn D, 'Intellectual Property Liability of Consumers, Facilitators, and Intermediaries: Concepts under Common Law' in Heath C and Sanders AK eds., *Intellectual Property Liability of Consumers, Facilitators, and Intermediaries* (Kluwer Law International 2012)
- Leistner M, 'Grundlagen und Perspektiven der Haftung für Urheberrechtsverletzungen im Internet', 2012 ZUM 731
- Lessig L, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 Harvard Law Review 501
- Lev-Aretz Y, 'Second Level Agreements' (2011) 45 Akron Law Review 137
- Lev-Aretz Y, 'Copyright Lawmaking and Public Choice: From Legislative Battles to Private Ordering' (2013) 27 Harvard Journal of Law & Technology 203
- Maxwell W, 'Systematic government access to private-sector data in France' (2014)

4 International Data Privacy Law 4
- Meliá JC, 'The Administrative and Judicial Procedure Concerning Internet Infringements: Much More Than a Simple Notice and Takedown Procedure' (2014), WIPO/ACE/9/21.
- Menasche NM, 'Recording Industry Missteps: Suing Anonymous Filesharers as a Last Resort' (2005), 26 Pace Law Review 273
- Merges RP, *Justifying Intellectual Property* (Harvard University Press. 2011)
- Merges RP, et al., *Intellectual Property in the New Technological Age: Case and statutory supplement* (Aspen Law & Business. 2005)
- Moore T and Clayton R, 'The impact of incentives on notice and take-down' in Johnson ME (eds), *Managing Information Risk and the Economics of Security* (Springer US 2009)
- Mousourakis G, 'Transplanting Legal Models across Culturally Diverse Societies: A Comparative Law Perspective' (2010) 57 Osaka University Law Review 87
- Netanel NW, 'Cyberspace Self-governance: A Skeptical View from Liberal Democratic Theory' (2000) 88 California Law Review 395
- Nimmer D, *Nimmer on Copyright*, (LexisNexis, 2013)
- Nimmer D, *Copyright: Sacred Text, Technology, and the DMCA*, (Kluwer Law International, 2003)
- Oswald LJ, 'International Issue in Secondary Liability for Intellectual Property Rights infringement' (2008) 45 American Business Law Journal 247
- Parti K and Marin L, 'Ensuring freedoms and protecting rights in the governance of the Internet: a comparative analysis of blocking measures of illegal Internet content and the liability of ISPs' (2013) 9 Journal of Contemporary European Research 138
- Peguera M, 'The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems' (2009) 32 Columbia Journal of Law & the Arts 481
- Ramalho A, 'The Competence of The European Union in Copyright Lawmaking – A Normative Perspective of EU Powers for Copyright Harmonization' (2014) University of Amsterdam
- Rantou MI, The growing tension between copyright and personal data protection on an online environment: The position of Internet Service Providers according to the European Court of Justice (2012) 3 European Journal of Law and Technology 2
- Reese RA, 'The Relationship Between the ISP Safe Harbors and Liability for Inducement' (2011) 8 Stanford Technology Law Review 1
- Ruse-Khan HG, 'Overlaps and Conflict Norms in Human Rights Law: Approaches of European Courts to Address Intersections with Intellectual Property Rights' in Geiger C (eds), *Research Handbook on Human Rights and Intellectual Property* (Edward Elgar Publishing, 2015)

- Sadeghi M, *The Knowledge Standard for ISP Copyright and Trademark Secondary Liability: A Comparative Study on the Analysis of US and EU Laws* (Brunel University London, 2013)
- Schuerman E, 'Internet Service Providers and Copyright Liability-Don't Touch... Or at Least Not Too Much: CoStar v. LoopNet' (2005), 30 Southern Illinois University Law Journal 573
- Scruers M, ' The History and Economics of ISP Liability for Third Party Content' (2002) , 88 Virginia Law Review 205
- Seidenberg S, 'Copyright in the Age of YouTube' (2009) 95 ABA Journal 46
- Seltzer W, 'Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment' (2010) 24 Harvard Journal of Law & Technology 171
- Shillito M and Meale D, 'Twentieth Century Fox Film Corp v Newzbin Ltd - copyright - online service provider held liable for copyright infringements of its users' (2010), 32 European Intellectual Property Review 67
- Simon AR, 'Contracting in the Dark: Casting Light on the Shadows of Second Level Agreements' (2014), 5 William & Mary Business Law Review 305
- Smith GJH and Boardman R, *Internet Law and Regulation* (Sweet & Maxwell. 2007)
- Spindler G and Leistner M, 'Secondary copyright infringement-New perspectives in Germany and Europe' (2006) 37 International Review of Intellectual Property and Competition Law 788
- Spindler G, et al., *Recht der Elektronischen Medien: Kommentar* (C.H. Beck. 2008)
- Spinello RA, *Regulating Cyberspace: The Policies and Technologies of Control* (Quorum Books. 2002)
- Starr P, 'The Meaning of Privatization' (1988) 6 Yale Law & Policy Review 6
- Sterling, JAL, *World Copyright Law*, (Sweet & Maxwell. 2008)
- Sullivan ER, 'Lost in Cyberspace: A Closer Look at ISP Liability' (2001) 12 Entertainment Law Review 192
- Szuskin L, et al., 'Beyond Counterfeiting: The Expanding Battle Against Online Piracy' (2009) 21 Intellectual Property & Technology Law Journal 4
- Tasillo A and Sterpi M 'Italy' in Calame TJ and Sterpi M eds., *Copyright Litigation: Jurisdictional Comparisons* (European Lawyer 2015)
- T. Kono, et al., *Selected Legal Issues of E-commerce* (Kluwer Law International. 2002)
- Urban JM and Quilter L, 'Efficient Process or Chilling Effects-Takedown Notices under Section 512 of the Digital Millennium Copyright Act' (2005) 22 Santa Clara High Technology Law Journal 621
- Van Gompel S, *Formalities in Copyright Law: An Analysis of Their History, Rationales and Possible Futures* (Kluwer Law International 2011)

- Vincents OB, 'When rights clash online: The tracking of P2P copyright infringements vs. the EC personal data directive' (2008) 16 International Journal of Law and Information Technology 270
- Waisman A and Hevia M, 'Theoretical Foundations of Search Eengine Liability' (2011) 42 International Review of Intellectual Property and Competition Law 785
- Wan Y, 'Safe Harbors from Copyright Infringement Liability in China' (2012) 60 Journal of the Copyright Society of the U.S.A 635
- Wang HC (王宏丞) and Cao LP (曹丽萍) and Li DT (李东涛), 'Study on the Key Points in the Cases of Infringement on Video-sharing Websites (论视频分享网站侵权案件中的焦点问题)' (2009) 4 Electronic Intellectual Property (电子知识产权) 11
- Wang Q and Guibault L, *Study on Online Copyright Regulation in China and Europe*, (Law Press 2008)
- Weatherall K, 'Of Copyright Bureaucracies and Incoherence: Stepping Back from Australia's Recent Copyright Reforms' (2007) 31 Melbourne University Law Review 967
- Williams KS, 'On-Line anonymity, deindividuation and freedom of expression and privacy' (2005) 110 Penn State Law Review 687
- Wu T, 'Tolerated Use' (2008) 31 Columbia Journal of Law & Arts 617
- Yen AC, 'Restoring the natural law: Copyright as labor and possession' (1990) 51 Ohio State Law Journal 517
- Zhang JH (张建华), *The Interpretation of Regulation on the Protection of the Right to Internet Dissemination of Information (信息网络传播权保护条例释义)* (China Legal Publishing House (中国法制出版社) 2006)

European Union Legislation and materials:

- Commission Staff Working Paper: Online Services, Including E-commerce, in the Single Market, SEC (2011) 1641 final, 11 January 2012
- Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L 178/1
- Council Directive 2001/29/EC of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society [2001] OJ L 167/10
- Council Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights [2004] OJ L 195/16
- Council Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic

communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105/54
- European Commission, European Governance – A White Paper (COM(2001) 428 final), Official Journal of European Communities, 2001/C 287/01.
- IP/97/313, Electronic Commerce: Commission Presents Framework for Future Action, 16 April 1997
- IP/98/999 'Electronic Commerce: Commission Proposes Legal Framework' 18 November 1998
- Maggiore M and Tardella E, 'Study on the conditions of claims for damages in case of infringement of EC competition rules – National Reports (Italy)' (2012), European Commission
- Nielson CK, Jervelund C, Pedersen KG, Rytz B, Hansen ES, Ramskov JL, 'Study on The Economic Impact of the Electronic Commerce Directive' (2007), European Commission, DG InternalMarket and Services Unit E2

Member States Legislation

- German Teleservices Act (1997)
- German Civil Code
- German Copyright Act
- German Criminal Procedure Code (Strafprozeßordnung, StPO)
- Gesetz über Urheberrecht und verwandte Schutzrecht e
- Telemediengesetz (TMG)
- UK Copyright, Designs and Patents Act
- Telemediengesetz (TMG)
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique
- The Electronic Commerce (EC Directive) Regulations 2002

The United States of America Legislation and materials:

- Congress, U. S., Digital Millennium Copyright Act, 105-304 (1998): 112
- Congress, U.S., House Report 105-796 (1997-1998)
- Congress, U. S., House Report 105-551 (1998), Part II 3
- Congress U.S., Senate Report, No. 105-190 (1998)
- Congress, U.S., United States Constitution (1887)
- Statement of Marybeth Peters, The Register of Copyrights before the Committee on the Judiciary (Intentional Inducement of Copyright Infringements Act of 2004), United States Senate, 108th Congress, 2nd Session, July 22, 2004.

China Legislation and materials:

- National People's Congress (全国人民代表大会), General Principles of the Civil Law of the People's Republic of China (中华人民共和国民法通则), Order No. 37 of the president of the People's Republic of China (中华人民共和国第37号主席令)
- National Copyright Office (国家版权局), Amending Draft of Copyright Law of the People's Republic of China (中华人民共和国著作权法修正草案), First Draft (March 2012); Second Draft (July 2012); Third Draft (June 2014)
- Standing Committee of the National People's Congress (全国人民代表大会常务委员会), Copyright Law of the People's Republic of China (中华人民共和国著作权法), Order No. 26 of the President of the People's Republic of China (中华人民共和国主席令第二十六号), February 26, 2010.
- State Council (国务院), People's Republic of China (中华人民共和国), Regulation on the Protection of the Right 0f Dissemination via Information network (信息网络传播权保护条例), Order No. 468 of the State Council (国务院 468号令), May 18, 2006.
- State Administration of Radio Film and Television; Ministry of Information Industry (国家广播电影电视总局; 信息产业部), Administrative Provisions for the Internet Audio-Video Program Service (互联网视听节目服务管理规定), Order No. 56 of the State Administration of Radio, Film and Television and the Ministry of Information Industry (国家广播电影电视总局、中华人民共和国信息产业部令第56号), December 20, 2007.
- Supreme People's Court (最高人民法院), Opinions of the Supreme People's Court on Certain Issues Concerning the Implementation of the "General Principles of the Civil Law of the People's Republic of China" (Trial) (最高人民法院关于贯彻执行《中华人民共和国民法通则》若干问题的意见（试行）), Fa (Ban) Fa [1998] No. 6 (法(办)发[1998]6号), January 26, 1988
- Supreme People's Court (最高人民法院), Interpretation of the Supreme People's Court on Certain Issues Related to the Application of Law in the Trial of Cases Involving Computer Network Copyright Disputes (最高人民法院关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释), Fa Shi [2000] No. 48 (法释[2000]48号), November 22, 2000.
- Supreme People's Court (最高人民法院), Interpretation of the Supreme People's Court on Certain Issues Related to the Application of Law in the Trial of Cases Involving Computer Network Copyright Disputes (最高人民法院关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释), Fa Shi [2006] No. 11 (法释[2006]11号), November 22, 2006
- Supreme People's Court, Provisions of the Supreme People's Court on Certain Issues Related to the Application of Law in the Trial of Civil Cases Involving Disputes over Infringement of the Right of Dissemination through Information Networks

(最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定), Fa Shi [2012] No. 20 (法释〔2012〕20号) November 26, 2012

- Beijing High People's Court (北京市高级人民法院), Opinions of Beijing High Court on Several Issues Concerning Disputes about Internet Copyright Infringements (trial) (北京市高级人民法院关于网络著作权纠纷案件若干问题的指导意（试行）), JingGaoFaFa[2010] No. 166 (京高法发[2010] 166号), May 19, 2010
- Beijing High People's Court (北京市高级人民法院), Guide for Hearing Copyright Disputes involving Video-sharing (视频分享著作权纠纷案件的审理指南), JingGaoFaFa[2012] No. 419 (京高法发[2012]419号)

International Legal Materials:

- Berne Convention for the Protection of Literary and Artistic Works (Berne Convention) of September 9, 1886, *available at* http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html (last visited 26-06-2013).
- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations General Assembly, A/66/290, 10 August 2011
- The Universal Declaration of Human Rights, United Nations General Assembly, 10 December 1948
- Agreement on Trade-Related Aspects of Intellectual Property Rights (Trips Agreement), Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization, signed in Marrakesh, Morocco on 15 April 1994, *available at* http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm (last visited 28-05-2013 2013).
- WIPO Copyright Treaty (WCT), adopted in Geneva on 20 December 1996, *available at* http://www.wipo.int/export/sites/www/treaties/en/ip/wct/pdf/trtdocs_wo033.pdf (last visited 29-04-2013).
- WIPO Performances and Phonograms Treaty (WPPT), adopted in Geneva on 20 December 1996, available at http://www.wipo.int/treaties/en/ip/wppt/trtdocs_wo034.html (last visited 29-08-2013).

Cases:
Cases in the EU

- Application nos. 3002/03 and 23676/03 *Times Newspapers Ltd (nos. 1 and 2) v. the United Kingdom* [2009] EMLR 14, ECHR.
- BGH, April 29, 2010, Case No. I ZR 69/08 – Vorschaubilder
- BGH, August 17, 2011, Case No. I ZR 57/09 - Stiftparfuem
- BGH, August 15, 2013, No. I ZR 80/12 n 67
- BGH: Verwendung fremder Fotografien für Rezeptsammlung im Internet – marions-kochbuch.de, 2010 NJW-RR 1276
- *Bunt v Tilley and others*, [2006] EWHC 407 (QB), para. 72
- Case C-275/06 *Productores de Música de España v Telefónica de España Sau ('Promusicae')* [2008] ECR I-00271
- Case C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH* [2009] ECR I-01227
- C-324/09, *L'Oréal SA and Others v eBay International AG and Others*, [2011] ECR I-06011
- Case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL ('SABAM')* [2011] ECR I-11959
- C-360/10, *SABAM v. Netlog NV* [2012], ECLI:EU:C:2012:85
- Case C-461/10, *Bonnier Audio AB v Perfect Communication Sweden AB* [2012] ECLI:EU:C:2012:2190
- Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH ('UPC Telekabel Wien')* [2014] ECLI:EU:C:2014:192
- *Credit Lyonnais Bank Nederland NV v. Export Credits Guarantee Dept* [1998] 1 Lloyd's Rep 19
- *Amstrad Consumer Electronics PLC v The British Phonographic Industry Limited* [1986] FSR 159
- *C.B.S. Songs Ltd and ors v. Amstrad Consumer Electronics Plc* [1988] 1 A.C. 1013.
- Joined Cases C-236/08 to C-238/08, *Google France SARL and Google Inc. v Louis Vuitton Malletier SA and Others,* [2010] ECR I-02417
- Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications and others* [2014] ECLI:EU:C:2014:238
- *Kaschke v Gray and Hilton*, Queen's Bench Division, [2010] EWHC 690 (QB)
- KG: Internetplattform zum Austausch von Fotodateien, 2010 MMR 203.
- LG Hamburg: Haftung eines Plattformbetreibers – YouTube, 2010 MMR 833
- LG Hamburg, Urteil vom 20.04.2012, 310 O 461/10
- *McGrath v Dawkins and Amazon*, [2012] EWHC B3 (QB)
- *Mitsui Limited v Nexen Petroleum UK Limited* [2005] EWHC 625 (Ch)
- OLG Düsseldorf, Urteil vom 31.03.2009, I-20 U 73/08

- OLG Hamburg, ZUM 2009, 642 – Pixum
- OLG München: Gewerbeschädigende Äußerungen in einem Meinungsforum im Internet, 2002 MMR 612
- Opinion of Advocate General, *L'Oreal v. eBay International AG*, case C-324/09
- *Tamiz v Google Inc.*, [2013] EWCA Civ 68
- *Twentieth Century Fox Film Corp v Newzbin Ltd*, [2010] EWHC 608 (Ch)

Cases in the US

- *Arista Records, Inc. v. Mp3Board, Inc.*, 2002 WL 1997918, 9 (S.D.N.Y. 2002)
- *Artista Records, LLC v. Does 1-12*, 2008 U.S. Dist. LEXIS 82548
- *Arista Records LLC v. Usenet.com, Inc.*, 633 F.Supp.2d 124, (S.D.N.Y.2009)
- *Arista Records LLC. v. Lime Group LLC*, 784 F. Supp. 2d 398, (S.D.N.Y. 2011)
- *Capitol Records, Inc. v. MP3tunes, LLC*, 821 F.Supp.2d 627, (S.D.N.Y., 2011)
- *Columbia Pictures Industries, Inc. v. Gary FUNG*, 2009 WL 6355911 (C.D. Cal.)
- *Columbia Pictures Industries, Inc. v. Gary FUNG*, 710 F.3d 1020, (9th Cir. 2013)
- *Corbis Corporation v. Amazon.com*, 351 F.Supp.2d 1090, (W.D. Washington 2004)
- *Costar Group Inc. v. Loopnet*, Inc., 164 F. Supp. 2d 688, (D. Md. 2001)
- *CoStar v. LoopNet*, 373 F.3d 544, (4th Cir. 2004)
- *Dudnikov v. MGA Entertainment, Inc.*, 410 F. Supp. 2d 1010 (D. Colo. 2005)
- *Elektra Records v. Gem Elec. Distribs*, 360 F. Supp. 821 (E.D.N.Y 1973)
- *Ellison v. Robertson*, 357 F3d 1072, (9th Cir, 2004)
- *Fonovisa v. Cherry Auction*, 76 F.3d 259, (9th cir. 1996)
- *Gershwin Publishing Corp. v. Columbia Artists Management, Inc.*, 443 F.2d 1159 (2d Cir. 1971)
- *Hendrickson v. Amazon.com, Inc.*, 298 F.Supp.2d 914 (C.D. Cal. 2003)
- *Hendrickson v. Ebay Inc.*, 165 F. Supp. 2d 1082, (C.D. Cal. 2001)
- *Io Group, Inc v. Veoh Networks, Inc.*, 586 Supp.2d 1132 (C.D.Cal. 2008).
- *In re Aimster Copyright Litigation*, 334 F.3d 643 (7th Cir. 2003)
- *Lenz v. Universal Music Corp.*, 572 F. Supp. 2d 1150 (N.D. Cal. 2008)
- *MGM Studio, Inc v. Grokster Ltd*, 380 F.3d 1154, (9th Cir. 2004)
- *MGM Studios Inc. v. Grokster Ltd.*, 545 U.S. 913 (2005)
- *M. Witmark & Sons v. Calloway*, 22 F.2d 412 (D. Tenn. 1927)
- *Online Policy Group v. Diebold Inc.*, 337 F. Supp. 2d 1195 (N.D.Cal. 2004)
- *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, (C.D. Cal. 2002)
- *Perfect 10, Inc. v. CCBill, LLC*, 340 F.Supp.2d 1077 (C.D. Cal. 2004)
- *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, (9th Cir. 2007)
- *Perfect 10, Inc. v. CCBill LLC*, 481 F.3d 751, (9th Cir, 2007)
- *Perfect 10, Inc. v. RapidShare*, No. 09-CV-2596 H (S.D. Cal., 2010).
- *Perfect 10, Inc. v. Google, Inc.*, No. CV 04-9484 AHM, 2010 WL 9479059 (C.D.

Cal. July 26, 2010)

- *Perfect 10, Inc. v. Giganews, Inc.*, 993 F. Supp. 2d 1192, (C.D. Cal. 2014)
- *Playboy Enterprises Inc. v. Frena*, 839 F.Supp. 1552 (M.D. Fla. 1993).
- *Religious Technology Center v. Netcom On-line Communications Services, Inc.* 907 F. Supp. 1361 (N.D. Cal. 1995)
- *RIAA v. Verizon Internet Services*, 240 F. Supp. 2d 24, (D.D.C. 2003)
- *RIAA v. Verizon Internet Services*, 257 F. Supp. 2d 244 (D.D.C. 2003),
- *RIAA v. Verizon Internet Services,* 351 F.3d 1229 (D.C. Cir 2003)
- *Rossi v. Motion Picture Ass'n of America*, 391 F.3d 1000 (9th Cir. 2004)
- *Sony Corp. of America. v. Universal City Studios*, 464 U.S. 417 (1984) n51
- *Tiffany (NJ) Inc. v. eBay, Inc.*, 600 F.3d 93, (2d Cir. 2010)
- *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022, at 1027 (9th Cir.2011)
- *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F.Supp.2d 1081 (C.D.Cal.2008)
- *United States v. Aina-Marshall*, 336 F.3d 167, (2d Cir. 2003)
- *United States v. Rodriguez*, 983 F.2d 455, (2d Cir.1993)
- *Viacom International, INC. v. YouTube, INC.*, 676 F.3d 19 (2nd Cir. 2012).
- *Viacom Int'l Inc. et al. v. YouTube et al.*, 07 civ. 2103 (LLS), 32 (S.D.N.Y. Apr. 18, 2013)

Cases in China

- *BuSheng v. YoBo (步升v.友播)*, Beijing Haidian District Court (北京市海淀区法院), No. 6939 Hai Min Chu Zi(2008) (（2008）海民初字第6939号)
- *chineseall.com v. 178.com (北京中文在线v.北京智珠网络技术)*, Beijing Chaoyang District Court (北京市朝阳区人民法院), No. 8854 Chao Min Chu Zi (2013) (（2013）朝民初字第8854号)
- *CiWen v. 56.com (慈文v.56网)*, Beijing Second Intermediate People's Court (北京市第二中级人民法院), No. 9 Er Zhong Min Zhong Zi (2008) (（2008）二中民终字第9号)
- *Fanya E-commerce v. Baidu.com (泛亚电子诉百度侵权信息网络传播权案)*, Beijing Higher Court (北京市高级人民法院), GaoMinChuZi No. 1201 ((2007)高民初字第1201号)
- *Guang Dian Wei Ye v. youku.com (广电伟业 v. 优酷)*, Beijing Haidian District Court (北京海淀区法院), (2008) Hai Min Chu Zi No. 9200 (2008海民初字9200).
- *Guang Dian Wei Ye v. youku.com (广电伟业 v. 优酷)*, Beijing Haidian District Court (北京海淀区法院), (2008) Hai Min Chu Zi No. 14023 (2008海民初字14023)
- *Han Han v. Baidu (韩寒诉百度)*, Beijing Haidian District Court (北京市海淀区

法院), No. 5558 Hai Min Chu Zi (2012) (2012海民初字第5558号)
- *Hua Xia Shu Ren v. Youku.com (华夏树人v.优酷)*, Beijing Haidian District Court (北京市海淀区法院), No. 9200 Hai Min Chu Zi (2008) (（2008）海民初字第9200号)
- *JiaHua Culture v. 56.com (佳华文化v.56网)*, Beijing Chaoyang District Court (北京朝阳地区法院), No.20595 Chao Min Chu Zi (2013) (（2013）朝民初字第20595号)
- *joy.cn v. 56.com (激动网v.56网)*, Beijing Haidian District Court (北京市海淀区法院), No. 24750 Hai Min Chu Zi (2008) (（2008）海民初字第6939号)
- *joy.cn v. 6room.com (激动网v.6房间)*, Beijing Haidian District Court (北京海淀区法院), (2008) Hai Min Chu Zi No. 22186 (2008海民初字9200)
- *joy.cn v. tudou.com (激动网v.土豆网)*, First People's Intermediary Court of Shanghai (上海市中级人民法院), (2009) HuYiZongMinWu(Zhi)ZhongZi No. 79 ((2009)沪一中民五(知)终字第79号)
- *joy.cn v. tudou.com (激动网v.土豆网)*, First People's Intermediary Court of Shanghai (上海市中级人民法院), HuYiZongMinWu(Zhi)ZhongZi No. 53 ((2009)沪一中民五(知)终字第53号);
- *joy.cn v. tudou.com (激动网v.土豆网)*, First People's Intermediary Court of Shanghai (上海市中级人民法院), HuYiZongMinWu(Zhi)ZhongZi No. 102 ((2009)沪一中民五(知)终字第102号).
- *Miao Fuhua v. 56.com (苗富华诉北京我乐信息科技有限公司等侵犯著作权纠纷案)*, Beijing Chaoyang District Court (北京市朝阳区人民法院), Chao Min Chu Zi No.30077 ((2011)朝民初字第30077号)
- *Ningbo Success Multi-media Telecom v. Yahoo.cn (宁波成功多媒体诉雅虎侵犯著作权纠纷案)*, Beijing Chaoyang District Court (北京市朝阳区人民法院), Chao Min Chu Zi No. 4679 ((2008)朝民初字第4679号)
- *nubb.com v. Tudou.com (新传在线v.土豆网)*, Shanghai High People's Court (*上海市高级人民法院*), No. 62 Hu Gao Min San (Zhi) Zhong Zi (2008) (（2008）沪高民三（知）终字第62号)
- *Qiao v. tiexue.net (乔某某 v. 铁血网)*, Beijing Haidian District Court (*北京市海淀区基层人民法院*), (2006) Hai Min Chu Zi, No. 15350 (（2006）海民初字第15350号)
- *Qiao v. china.com (乔某某 v. 中华网)*, Beijing Second Intermediate People's Court (*北京市海淀区中级人民法院*), (2006) Er Zhong Min Chu Zi, No. 8997 (（2006）二中民初字第8997号)
- *Qiao v. china.com (乔某某 v. 中华网)*, Beijing Second Intermediate People's Court (*北京市海淀区中级人民法院*), (2006) Er Zhong Min Chu Zi, No. 8997 (（2006）二中民初字第8997号)
- *3rd Mian Xiang v. Great Wall Broadband (三面向诉长城宽带)*, Hubei Wuhan Intermediate People's Court (湖北省武汉市中级人民法院), (2009) Wu Zhi Chu

Zi, No. 18 ((2009)武知初字第18号)
- *Universal Music v. Yahoo.cn (环球唱片诉雅虎侵犯信息网络传播权案)*, Beijing Second Intermediate Court (北京市第二中级人民法院), ErZhongMinChuZi No. 02622 ((2007)二中民初字第02622号)
- *vale.com v. tudou.com (网乐互联v.土豆网)*, Shanghai First Intermediate People's Court (上海市第一中级人民法院), No. 19 Hu Yi Zhong Min Wu (Zhi) Zhong Zi (2009) (（2009）沪一中民五（知）终字第19号)
- *Wangyajun v. Lingshida Tech. (王亚军v.北京零时达科技)*, Beijing Haidian District Court (北京市海淀区人民法院), No. 2775 Hai Min Chu Zi (2008) (（2008）海民初字第2775)
- Yinian v. Taobao (衣念v.淘宝), Shanghai First Intermediate People's Court (上海市第一中级人民法院), No. 40 Hu Yi Zhong Min Wu (Zhi) Zhong Zi (2011) (（2011）沪一中民五（知）终字第40号)
- ZhongQinWen v. Baidu (中青文v.百度), Beijing First Intermediate People's Court (北京市第一中级人民法院), (2013)YiZhongMinChuZi, No. 11912 (（2013）一中民初字第11912号)
- *ZhongQinWen v. Baidu (中青文v.百度)*, Beijing High People's Court (北京市高级人民法院), 2014 GaoMinZhongZi, No. 2045, (（2014）高民终字第2045)号

Internet materials:

- *101 websites sign in "Self-discipline Declaration on Copyright Protection by Internet Industry in China" together (101家网站共同发布《中国互联网行业版权自律宣言》)*, www.npc.gov.cn (全国人大网)(2010), *available at* http://www.npc.gov.cn/npc/xinwen/fztd/fzsh/2010-01/21/content_1535617.htm (last visited 12-12-2014)
- Ahlert C, et al., How 'liberty' disappeared from cyberspace: the mystery shopper tests Internet content self-regulation (2004), RootSecure.com, available at http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf (last visited 08-12-2014)
- *A clean and open Internet: Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries*, European Commission(2012), *available at* http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-internet_en.htm (last visited 19-02-2014)
- Amélie Blocman, Liability of Video-sharing Platforms - First Judgement of Court of Cassation, *available at* http://merlin.obs.coe.int/iris/2011/3/article18.en.html [last visited July 26, 2013]
- Barnes B and Stone B, *MGM to Post Full Films on YouTube*, The New York Time(2008), *available at* http://www.nytimes.com/2008/11/10/business/

media/10mgm.html?_r=2& (last visited 12-12-2014)
- Blocman A, *Liability of Video-sharing Platforms - First Judgement of Court of Cassation*, IRIS Merlin(2011), *available at* http://merlin.obs.coe.int/iris/2011/3/article18.en.html (last visited 03-08-2014)
- Bulletin board system, Wikipedia, *available at* https://en.wikipedia.org/wiki/Bulletin_board_system (last visited 09-02-2014)
- CBS and Youtube Strike Strategic Content And Advertising Partnership, CBS Corporation (2006), *available at* http://www.cbscorporation.com/news-article.php?id=23 (last visited 09-02-2013)
- Chiang O, *Justin Bieber Swears Off YouTube For Facebook, Unwittingly Steps In Copyright Minefield*, Forbes(2010), *available at* http://www.forbes.com/sites/oliverchiang/2010/11/30/justin-bieber-swears-off-youtube-for-facebook-unwittingly-steps-in-copyright-minefield/ (last visited 12-16-2014).
- *Content Identification Application*, YouTube, *available at* https://www.youtube.com/content_id_signup (last visited 12-24-2014).
- Coraggio G, *YouTube case changes rules on Internet liability*, Lexology(2014), *available at* http://www.lexology.com/library/detail.aspx?g=bf912a7f-b3d2-47b2-9fed-c50534122b00 (last visited 26-04-2014)
- Crossley R, *Industry fights back as YouTube begins mass cull of game videos*, CVG(2013), *available at* http://www.computerandvideogames.com/442245/industry-fights-back-as-youtube-begins-mass-cull-of-game-videos/ (last visited 12-16-2014).
- David Lizerbram, *Using Copyright to Suppress Criticism?*, David Lizerbram & Associates(2014), *available at* http://lizerbramlaw.com/2014/08/using-copyright-suppress-criticism/, (last visited 25-09-2014).
- Fair Use Principles for User Generated Video Content, Electronic Frontier Foundation (2007), *available at* https://www.eff.org/pages/fair-use-principles-user-generated-video-content (last visited 28-07-2014)
- Fahllund K, *Country Report (Finland)*, Global Advertising Lawyers Alliance(2002), *available at* http://www.gala-marketlaw.com/pdf/finland2002.pdf (last visited 20-08-2014)
- Fitzgerald B, *YouTube Pulls Michelle Obama's Democratic National Convention Speech In 'Error'*, The Huffington Post(2012), *available at* http://www.huffingtonpost.com/2012/09/05/youtube-pulls-michelle-obama-speech_n_1857708.html (last visited 12-16-2014).
- Gray ME, *FatWallet Victorious in Challenge to Wal-Mart's Frivolous DMCA Subpoena*, BerkleyLaw(2002), *available at* http://www.law.berkeley.edu/4719.htm (last visited 20-08-2014)
- Higgins P, *YouTube Upgrades Its Automated Copyright Enforcement System*, Electronic Frontier Foundation(2012), *available at* https://www.eff.org/deeplinks/2012/10/youtube-upgrades-its-automated-copyright-enforcement-system (last visited 12-16-2014)

- Higgins P, *Mars Landing Videos, and Other Casualties of the Robot Wars*, Electronic Frontier Foundation(2012), *available at* https://www.eff.org/deeplinks/2012/08/mars-landing-videos-and-other-casualties-robot-wars (last visited 12-16-2014)
- Holger Schmidt, *Die Antwort auf Youtube: Universal-Musikvideos jetzt auf Sevenload*, Frankfurt Allemeine(2009), *available at* http://blogs.faz.net/netzwirtschaft-blog/2009/04/02/die-antwort-auf-youtube-universal-musikvideos-jetzt-bei-sevenload-1014/ (last visited 12-16-2014)
- Holland CBA, Hermes J, Sellars A, Budish R, Lambert M, and Decoster N, *NoC Online Intermediaries Case Studies Series: Intermediary Liability in the United States at* http://cyber.law.harvard.edu/is2015/sites/is2015/images/NOC_United_States_case_study.pdf (last visited 28-09-2014)
- Instruction about How to Fill in "the Notice requiring the deletion of or cutting off the links to infringing materials" (《要求删除或断开链接侵权网络内容的通知》填写说明), http://www.ncac.gov.cn/chinacopyright/contents/574/20879.html, (last visited 14-11-2014)
- Jasserand C, *France- Dailymotion heavily fined for the late removal of infringing content*, wolters kluwer law & business(2012), *available at* http://kluwercopyrightblog.com/2012/09/28/france-dailymotion-heavily-fined-for-the-late-removal-of-infringing-content/, (last visited 28-09-2014).
- Jasserand C, *France -Youtube guilty but not liable? some more precisions on the status of hosting providers*, wolters kluwer law & business(2012), *available at* http://kluwercopyrightblog.com/2012/06/18/france-youtube-guilty-but-not-liable-some-more-precisions-on-the-status-of-hosting-providers/, (last visited 28-09-2014).
- Kim Zetter, *Yahoo Issues Takedown Notice for Spying Price List*(2009), *available at* http://www.herbogeminis.com/IMG/pdf/yahoo.pdf, (last visited 26-08-2014)
- Lattman P, *Law Professor Wendy Seltzer Takes on the NFL*, Law Blog - WSJ.com(2007), *available at* http://blogs.wsj.com/law/2007/03/21/law-professor-wendy-seltzer-takes-on-the-nfl/. (last visit 25-08-2014)
- Leger P, *Internet Service Providers' liability in France*, CERDI(2012), *available at* https://www.google.nl/l?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0CCwQFjAC&url=http%3A%2F%2Fwww.cerdi.u-psud.fr%2Fwp-content%2Fuploads%2F2013%2F05%2FInternet-service-providersliability-in-France-P-Leger.pptx&ei=K33eVKi1J4SfPayYgPAM&usg=AFQjCNGmn-YXh1IrydyS1MoV8I51HEwRVQ&sig2=wSi5ADRPXJh7jgnS1I0yeQ&bvm=bv.85970519,d.d2s (last visited 12-08-2014)
- Lucy Nunn, *Internet service providers: copyright infringement*, Thomson Reuters(2014), *available at* http://login.westlaw.co.uk/maf/wluk/app/document?src=doc&linktype=ref&context=23&crumb-action=replace&docguid=I4B88A580587211E4B6DA87DCBE8E5CD8 (last visited 14-05-2014)

- McKay P, *YouTube Copyfraud & Abuse of the Content ID System*, Fair Use Tube(2012), *available at* http://fairusetube.org/youtube-copyfraud (last visited 12-23-2014)
- Miguel Helft, *Google told to turn over user data of YouTube*, The New York Times(2008), *available at* http://agriculturedefensecoalition.org/sites/default/files/file/constitution_1/1G_2008_Viacom_Lawsuit_Google_YouTube_July_4_2008_NYTimes.pdf, (last visited 20-08-2014)
- *Music Publisher Tries to Muzzle Podcast Criticizing Akon*, Electronic Frontier Foundation(2007), *available at* https://www.eff.org/takedowns/music-publisher-tries-muzzle-podcast-criticizing-akon
- *Notice-and-Take-Down Code of Conduct*, ecp.nl(2008), *available at* http://ecp.nl/over-ecp/216/over-ecp.html (last visited 15-12-2014)
- *Press Conference on 2009 Special Action held by State Administration of Press and Publication(新闻出版总署2009专项行动新闻发布会)*, http://www.scio.gov.cn/(2010), *available at* http://www.scio.gov.cn/wlcb/blxxjbygl/Document/527754/527754.htm (last visited 20-12-2014)
- Principles for User Generated Content Services (2007), *available at* http://www.ugcprinciples.com/ (last visited 12-06-2015)
- Privacy and Data Protection, Council of Europe, *available at* http://www.coe.int/en/web/internet-users-rights/privacy-and-data-protection (last visited 12-08-2014)
- Paul Roberts, *Diebold Voting Case Tests DMCA*, PCWorld(2003), *available at* http://www.pcworld.com/article/113273/article.html (last visited 27-11-2014).
- *Qualifying for Content ID*, YouTube, *available at* https://support.google.com/youtube/answer/1311402?hl=en (last visited 12-16-2014).
- Self-discipline Treaty on Internet Audio-video Program Services in China (中国互联网视听节目服务自律公约), State Administration of Radio Film and Television (国家广电总局)(2008), *available at* http://www.sarft.gov.cn/articles/2008/02/22/20080226114116260491.html (last visited 16-06-2015)
- Shanshan Wang (王珊珊), *"Cat-Mouse Game" between Chinese Video-sharing Websites and State Administration of Radio, Film and Television (中国视频网站与广电总局的"猫鼠游戏")*, The New York Times 纽约时报中文网(2014), *available at* http://cn.tmagazine.com/film-tv/20140430/tc30shows/ (last visited 12-16-2014).
- Sony BMG Music Entertainment Sighs Content License Agreement with YouTube, Sony Music(2006), *available at* http://www.sonymusic.com/sonymusic/sony-bmg-music-entertainment-signs-content-license-agreement-with-youtube/ (lasted visited 13-09-2013)
- Spedicato G, *Italy: the take-down notice must contain the specific YouTube URLs*, Wolters Kluwer(2014), *available at* http://kluwercopyrightblog.com/2014/05/28/italy-the-take-down-notice-must-contain-the-specific-youtube-urls/ (last visited 27-08-2014)
- Spitz B and Avocats YS, *France: Radioblog condemned to damages for over €1 million*,

Wolter Kluwer(2012), *available at* http://kluwercopyrightblog.com/2012/11/13/france-radioblog-condemned-to-damages-for-over-e1-million/ (last visited 27-08-2014).

- Spongeyday, *Who is WMG and why are they claiming certain songs to be "Unauthorized"?* , YouTube Help Forum(2010), *available at* https://productforums.google.com/forum/?hl=en#!category-topic/youtube/feedback--suggestions/DEtO1hFLXMM (last visited 12-16-2014)
- Statistics, YouTube(2015), *available at* http://www.youtube.com/yt/press/statistics.html (last visited 21-09-2015)
- Stephen W. Workman, Internet Law - Developments in ISP Liability in Europe, *available at* http://www.ibls.com/internet_law_news_portal_view.aspx?id=2126&s=latestnews [last visited July 26, 2013]
- Steve Chen, *The state of our video ID tools*, Google Offical Blog(2007), *available at* http://googleblog.blogspot.nl/2007/06/state-of-our-video-id-tools.html (last visited 12-24-2014).
- Targeted advertising, Wikipedia, *available at* http://en.wikipedia.org/wiki/Targeted_advertising (last visited 12-09-2014)
- YoukuTudou signed a 5-year copyright licensing contract with Sony Picture (优酷土豆与索尼音像签订五年版权协议), it.sohu.com(2012), *available at* http://it.sohu.com/20121106/n356832451.shtml (lasted visited 18-09-2013)
- *Youku Copyright Cooperation System (优酷版权合作协议)*, Youku, *available at* http://www.youku.com/copyright_apply.html (last visited 12-24-2014)
- YouTube also establishes its own filtering system named "Content ID", see How Content ID works, *available at* https://support.google.com/youtube/answer/2797370?hl=en (last visited 18-06-2015)
- United States, Electronic Frontier Foundation, available at https://www.eff.org/issues/mandatory-data-retention/us (last visited 20-08-2014)
- Universal Music Group and YouTube Forge Strategic Partnership, Universal Music Group(2006), *available at* http://www.universalmusic.com/corporate/detail/393 (lasted visited 13-09-2013)
- *Universal Music Group Backs Off Claims to Michelle Malkin Video*, Electronic Frontier Foundation(2007), *available at* https://www.eff.org/deeplinks/2007/05/universal-music-group-backs-claims-michelle-malkin-video (last visited 25-09-2014)
- Verbiest T et al., Study on the Liability of Internet Intermediaries (2007), *available at* http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf (last visited 28-08-2015)
- Warner Music Group and YouTube Announce Landmark Video Distribution and Revenue Partnership, Warner Music Group(2006), *available at* http://investors.wmg.com/phoenix.zhtml?c=182480&p=irol-newsArticle&ID=906153 (last visited

09-02-2013)

- Workman SW, Internet Law - Developments in ISP Liability in Europe, IBLS, *available at* http://www.ibls.com/internet_law_news_portal_view.aspx?id=2126&s=latestnews (last visited 01-03-2014)

Summary

Hosting ISPs' services are featured with duel uses, which means their services can be used for both infringing and non-infringing purposes. In practice, many users upload materials copyrighted by others on hosting platforms without authorization, and a large number of these uploadings constitute copyright infringement. Because it is very much less cost-effective for copyright owners to sue Internet users who directly commit copyright infringement, copyright owners turn to hosting ISPs and request them as gatekeepers to be responsible for copyright infringement on their platforms. In the US, EU and China, lawsuits between copyright owners and hosting ISPs have occurred on a tremendous scale, which poses obstacles for hosting ISPs to conduct business in these jurisdictions. For these hosting ISPs which are operating or planning to operate in the US, EU and China, it is necessary to know the legal risks they face and then adapt their ways of operation so as to avoid these legal risks. Further, in order to ensure the freedom to operate of hosting ISPs, it is also necessary to examine whether current rules that regulate hosting ISPs' responsibilities for copyright infringement impose an unreasonable burden on them, and if the answer is "yes", how should current responsibility rules be adjusted so as to avoid imposing such an unreasonable burden, or is there any other way which can better regulate hosting ISPs' responsibilities for copyright infringement? In addition, the Internet is borderless, so hosting ISPs naturally have the advantage to conduct international business, but this advantage can decline if lacking the harmonization of rules that regulate their responsibilities for copyright infringement at the international level. In the US, EU and China, "safe harbor" provisions which grant hosting ISPs liability exemption under certain circumstances have been commonly adopted, so in this respect, a certain degree of harmonization has been reached. Nevertheless, the liability rules in the US, EU and China are diverse, and the courts in these jurisdictions tend to interpret "safe harbor" provisions in different ways, so hosting ISPs still face a high level of legal uncertainty when expanding their business in these jurisdictions. Therefore, it is necessary to check whether and how further harmonization can be achieved at the judicial level in the US, EU and China.

Based on the above observations, Chapter 1 first narrates some background information of this study. Then it presents the research question: how to regulate hosting ISPs' responsibilities for copyright infringement while preserving their maximum freedom to operate in the US, EU and China? Thereafter, it introduces the methodology and outline of this study.

Chapter 2 narrates the rules that regulate hosting ISPs' responsibilities for copyright infringement in the US, EU and China, including the liability rules relevant to decide indirect copyright infringement and "safe harbor" provisions. It concludes that in the US, EU and China, the rules of indirect copyright infringement are diverse, but the liability exemption rules are substantially similar. Further, "safe harbor" provisions play an important role in regulating hosting ISPs' responsibilities for copyright infringement.

The introduction of responsibility rules in this Chapter provides the basis for the analysis of relevant case law in the next four chapters.

In the light of "safe harbor" provisions, hosting ISPs need to keep passive in operation so as to fall under "safe harbor". Chapter 3 takes a comparative approach to examine how the courts in the US, EU and China interpret "keeping passive" in case law. Based on the examination of case law, it summarizes the circumstances in which courts hold hosting ISPs not qualifying for keeping passive, and they are: commercially exploiting the uploaded content, editing or categorizing the uploaded content, displaying its logo with uploaded content, requiring rights transfer by "terms and conditions," and uploading some content by itself. Then, it concludes that these circumstances should not exclude hosting ISPs from "safe harbor" provisions, except editing, categorizing or actively exploiting the uploaded contents. Finally, this chapter asserts that it is unreasonable to require hosting ISPs to keep purely passive anymore. In order to preserve maximum freedom for hosting ISPs to operate, the following two criteria ought to be employed when deciding whether the management done by hosting ISPs is permissible: (1) check whether this management will result in a hosting ISP's knowledge or control of uploaded content, (2) whether this management is conducive to preventing infringements or not.

Once hosting ISPs fall under "safe harbor", they still need to meet the prescribed conditions so as to be exempted from liability. Chapter 4 explores how the courts in the US, EU and China decide hosting ISPs' copyright liability under the roof of "safe harbor" provisions. Generally, the courts evaluate the following factors: (1) hosting ISPs are not obligated to undertake general monitoring responsibility; (2) whether hosting ISPs have specific knowledge of infringement; (3) whether hosting ISPs take reasonable measures against repeat infringement; (4) whether hosting ISPs benefit from infringement; (5) whether hosting ISPs induce infringement, or intend to facilitate infringement. In the light of case law, factors (3) and (5) become much more important in deciding whether hosting ISPs are liable. Regarding factor (3), Chapter 4 asserts, specific monitoring against repeat infringement should not be defined as an obligation but rather a positive factor to grant hosting ISPs liability exemption. Regarding factor (5), Chapter 4 concludes that only when a hosting ISP bears a specific intent to induce copyright infringement, should it be held liable. Through interpreting factors (3) and (5) in these ways, it helps to preserve maximum freedom for hosting ISPs to operate in the US, EU and China.

Besides being subject to copyright liability under certain circumstances, hosting ISPs are also obligated to fulfill certain duties to facilitate copyright protection on their platforms. Chapters 5 and 6 explore the notice-and-takedown procedures and identity disclosure mechanism respectively. In the light of notice-and-takedown procedures, hosting ISPs need to expeditiously remove the alleged infringing materials upon receiving competent notices. Based on the examination of case law, Chapter 4 summarizes the main questions

that need to be dealt with by courts when ruling on notice-and-takedown procedures, and then concludes how these questions ought to be answered from the perspective of preserving hosting ISPs' freedom to operate. These questions are as follows: how to define a competent notice, how to deal with the defect notices, how to define "expeditiously remove", how to regulate the liability of wrong deletion, and the validity of ex ante notices. Overall, in notice-and-takedown procedures, copyright owners ought to shoulder the responsibility of seeking and identifying infringing materials, and the duty of hosting ISPs is to help copyright owners protect their rights, such as expeditiously removing the suspected infringing materials after receiving notices. Further, hosting ISPs also function as a communication conduit between copyright owners and Internet users, such as forwarding notices and counter notices. Regarding wrong deletion, more duties should be imposed upon copyright owners rather than on hosting ISPs in order to reduce it.

According to identity disclosure mechanisms, hosting ISPs are obligated to disclose the infringers' identities under certain circumstances. Based on the examination of identity disclosure mechanisms in the US, EU and China, Chapter 6 concludes that hosting ISPs' duties are mainly based on the answers to these two questions: (1) under what circumstances is a hosting ISP obligated to conduct disclosure; (2) to what extent should a hosting ISP disclose a suspected infringer's identity. Generally, hosting ISPs assume a passive obligation in identity disclosure mechanisms, and that is to disclose the identity information of alleged infringers to the extent that such information is available to them, upon receiving orders from competent third parties. Further, they are not responsible for the failure of identifying suspected infringers once they disclose the identity information retained by them. In addition, hosting ISPs should be forbidden to disclose their users' identity information to copyright owners without court orders. These duties require a little effort to fulfill, and do not unreasonably restrict hosting ISPs' freedom to operate. The disputes between copyright owners and hosting ISPs have not been solved through state regulation, so at private level, they start to cooperate and reach self-regulation so as to reduce the endless lawsuits. Chapter 7 explores two types of self-regulation which are codes of conduct and second level agreements. Compared with state regulation regimes, self-regulation can better preserve the freedom for hosting ISPs to operate. Within a self-regulation regime, hosting ISPs face more legal certainty in operation. Further, self-regulation can avoid imposing unreasonable burdens on hosting ISPs, and even entitle more freedom to hosting ISPs to commercially exploit the content on their platforms. Nevertheless, the applicability of self-regulation is limited, and particularly, small hosting ISPs have little chance join the self-regulation agreements controlled by several dominating market players. Further, self-regulation is generally the "best practice" reached between copyright owners and hosting ISPs, and may put Internet users' interests in danger. From the legal perspective, hosting ISPs can usually avoid being held liable for endangering Internet users' interests, because Internet users

need to agree with the "terms of services" before using the services, and the "terms of services" grant wide rights and liability exemptions to hosting ISPs. Nevertheless, the measures taken by hosting ISPs should avoid violating the mandatory norms which aim at protecting Internet users' interests.

Finally, Chapter 8 summarizes and assesses the research findings in previous chapters, and then answers the main research question and sub-research questions. In addition, it also provides some recommendations for hosting ISPs who are currently conducting business or planning to operate in the US, EU and China. Furthermore, it addresses the limitations of this research and points out what could be done in the future.

Valorization Addendum

1 Social and Economic Relevance

How to define hosting ISPs' responsibilities for copyright infringement on their platform has become an increasingly important issue in our society. In the last decade, with the development of information technologies, the services offered by hosting ISPs have been steadily updated. Because hosting ISPs' services are featured with dual-use, the update of hosting services not only helps the public to access lawful information more conveniently, but also allows copyrighted materials to be more easily shared and accessed without authorization. Copyright owners claim that copyright infringement on hosting platforms causes tremendous damage to them, and therefore request hosting ISPs to undertake more responsibilities to reduce copyright infringement. By contrast, hosting ISPs argue that imposing too many copyright responsibilities on them would stifle their freedom to operate. In the US, EU and China, lots of litigations have occurred between copyright owners and hosting ISPs, and different courts tend to interpret responsibility rules in different ways, which results in different impacts on hosting ISPs' freedom to operate.

How much freedom hosting ISPs should have in operation is a question which generates substantial effect on **e-commence**. The business engaged by hosting ISPs accounts for an important part in e-commerce. The hosting ISPs like YouTube, Facebook and eBay have been playing a leading role in e-commerce. Therefore, in order to promote

the development of e-commerce, it is necessary to avoid imposing too burdensome copyright responsibilities on hosting ISPs so as to ensure their freedom to operate. If the legal risks faced by hosting ISPs are too high, there will be much less investment being poured in this sector, which is detrimental to e-commerce. First, technology innovators will lack incentives to develop and implement new technologies which can optimize their hosting services. Second, investors will reduce their capital investment in the hosting service industry because of the dim prospects to make profits. In the US, EU and China, although "safe harbor" provisions have been commonly adopted to ensure hosting ISPs' freedom to operate, the courts in these jurisdictions have developed several liability criteria which may impose too far-reaching obligations on hosting ISPs. These far-reaching obligations to a large extent increase the legal risks faced by hosting ISPs in operation. Particularly, for many start-up hosting ISPs, they may be not capable of fulfilling these obligations. This study examines the responsibility rules in the US, EU and China, and then suggests how these responsibility rules ought to be adjusted so as to avoid imposing unreasonable burden on hosting ISPs.

Benefiting from the borderless Internet, hosting ISPs naturally have the advantages to expand their business into other countries. However, in different jurisdictions, hosting ISPs are subject to different copyright responsibilities, which causes legal uncertainty for those hosting ISPs who operate internationally, and thus poses obstacles to the development of **cross-border** e-commerce. This study examines the legislations and

case law relevant to regulating hosting ISPs' responsibilities for copyright infringement, and then draws the copyright responsibilities imposed on hosting ISPs in the US, EU and China, which helps hosting ISPs map their legal risks in these jurisdictions. After knowing the legal risks, hosting ISPs can more easily make their business plans when operating in the US, EU and China. In addition, for the purpose of promoting cross-border e-commerce, it would be quite helpful to harmonize the rules that regulate hosting ISPs' copyright responsibilities in different jurisdictions. Currently, the "safe harbor" provisions are per se homogenous in the US, EU and China, so in this regard, certain harmonization has been achieved in regulating the copyright responsibilities of hosting ISPs. This study examines how the "safe harbor" provisions are interpreted by the courts in the US, EU and China, and then discusses whether and how further harmonization can be done in respect of interpreting "safe harbor" provisions.

With the development of information technologies, nearly all kinds of works, including books, music, movies, games and software, can easily be uploaded on hosting platforms without authorization. Copyright owners complain that infringement on hosting platforms results in huge damage on the **copyright industry**. This study bears in mind that hosting ISPs' freedom to operate should be restricted by copyright protection, and it is necessary to require hosting ISPs to undertake certain responsibilities for reducing copyright infringement on their platforms. In addition, this study also explores the self-regulation between copyright owners and hosting ISPs, and demonstrates how to reach mutually beneficial agreements regarding dealing with infringing materials on hosting platforms.

The copyright responsibilities imposed on hosting ISPs also affect the **Internet users' freedom of expression**. The services offered by hosting ISPs help Internet users access knowledge and information immensely. It is quite convenient for Internet users to find the information they need on hosting platforms. In addition, with the help of services offered by hosting ISPs, Internet users can not only passively receive the information they need, but also can actively engage in generating and distributing information. For instance, video-sharing websites like YouTube and Dailymotion not only allow Internet users to listen to music, watch and movies, but also allow them to share the videos generated by them with others; social networking platforms like Facebook and Twitter allow Internet users to post their opinions online and exchange their ideas with others. Therefore, the services offered by hosting ISPs enlarge the public's ability to the freedom of expression. If imposing too many copyright responsibilities on hosting ISPs, hosting ISPs may be forced to shut down their services, and there will be fewer hosting services that allow Internet users to access, generate and distribute information. Moreover, facing too high a level of legal risk, hosting ISPs may over-react towards the materials uploaded by Internet users, which causes lots of lawful materials to be taken down. This study recommends how to preserve maximum freedom for hosting ISPs to operate, which can generate a positive externality on Internet users' freedom of speech.

2 Target Groups

The results of this study should be interesting to various groups, including academics and practitioners, who are engaged in dealing with hosting ISPs' copyright responsibilities. This thesis takes a comparative approach to study the hosting ISPs' copyright responsibilities in the US, EU and China. The comparison covers the legislation, case decisions and self-regulation agreements, which could offer useful clues for **legislators** to revise the current law, for **judges** to decide the cases about hosting ISPs' copyright responsibilities, and for **copyright owners** and **hosting ISPs** to lay down their market plans.

All of the US, EU and China adopt "safe harbor" provisions at legislative level, which grant hosting ISPs liability exemption under certain conditions while requiring them to undertake certain duties so as to facilitate copyright enforcement on hosting platforms. In this regard, the laws that regulate hosting ISPs' copyright responsibilities are per se homogenous. Nevertheless, the norms provided by the "safe harbor" provisions in these jurisdictions are not the same. This study compares these different norms and finds out the different impacts resulting from these norms in practice. These findings can help legislators evaluate whether the norms concerned need to be revised and how to revise these norms.

Judges may also be interested in reading this thesis. Since the "safe harbor" provisions in the US, EU and China are per se homogenous, judges in one jurisdiction may want to know how the courts in other jurisdictions interpret the similar norms concerned. This thesis looks into the case law about deciding the copyright responsibilities of hosting ISPs in the US, EU and China. Regarding whether hosting ISPs should be held liable for the infringing materials on their platforms, this study examines how the courts in the US, EU and China evaluate the factors relevant to conclude liability, including knowledge of infringement, benefiting from infringement, inducement and measures against repeat infringement. Regarding the notice-and-takedown procedure, this study examines how the courts in the US, EU and China decide some key issues, including how to define a competent notice, how to deal with the defect notices, how to define "expeditiously remove", how to regulate the liability of wrong deletion, and the validity of ex ante notices. In addition, this study also concludes how these disputed factors ought to be interpreted for the purpose of better preserving the freedom to operate of hosting ISPs, which may also provide useful clues for courts to decide cases that concern hosting ISPs' copyright responsibilities.

The result of this study should be of interest to copyright owners and hosting ISPs. This thesis not only examines the norms of hosting ISPs' copyright responsibilities at legislative level in the US, EU and China, but also examines how the courts in these jurisdictions interpret these norms when hearing relevant cases. From the perspective of copyright owners, the result of this study can help them evaluate the responsibility

norms in the US, EU and China, and then decide whether to sue hosting ISPs and choose the most suitable litigation strategies in these jurisdictions. From the perspective of hosting ISPs, the result of this study can help them evaluate the legal risks of conducting business in the US, EU and China, and then take the corresponding measures to reduce the legal risks they face in these jurisdictions. In addition, this study also covers the self-regulation agreements reached between copyright owners and hosting ISPs. These self-regulation agreements demonstrate how copyright owners and hosting ISPs cooperate with each other and solve the copyright disputes on hosting platforms. Copyright owners and hosting ISPs can learn from these self-regulation agreements, and reach similar agreements so as to settle the disputes between them.

3 Activities and Products

The result of this study will be published as a book. Therefore, it will be available to the people including students, academics, judges, legislators, policy makers, copyright owners and hosting ISPs who are interested in the topic of how to regulate hosting ISPs' responsibilities for copyright infringement. By reading this book, students and academics can know the rules of hosting ISPs' copyright responsibilities at both legislative and case law levels, and based on this knowledge, they can develop their own arguments and ideas on regulating the copyright responsibilities of hosting ISPs. In addition, this study also points out that some provisions in legislation need to be revised, and these recommendations may be considered by legislators. Besides, this study gives some recommendations on how to interpret current rules when deciding hosting ISPs' copyright responsibilities, which can be adopted by judges. Finally, as has already been mentioned above, copyright owners and hosting ISPs can make their litigation strategies by referring to this study.

Parts of this study have been published in academic journals. For instance, Chapter 3 has been published in European Intellectual Property Review, and parts of Chapter 4 related to the US, Germany and China have been published in International Review of Intellectual Property and Competition Law. Further, parts of this study are results of the research projects that the author was engaged in. For instance, Part of Chapter 5 in relation to the EU and China is an updated version of a report submitted to China-EU Law School (Research project: "A Comparative Study on Secondary Liability of Hosting ISPs"). Part of Chapter 6 in relation to China is an updated version of a research report submitted to Google and University of Washington (Research Project: "UW-Google Intermediary Liability Research Project"). Chapter 7 is an updated version of a conference paper "Self-regulation: a New Way against Copyright Infringement on UGC Websites" which was presented at the "Intellectual Property Work-in-Progress Colloquium" held in the University of Washington. The feedback from other experts

made a great contribution to the improvement of this research.
Under the support of CESL (China-EU School of Law) and Prof. A.W.J. Kamperman Sanders, the author held a workshop "Secondary liability of hosting Internet Service Providers in the European Union" at the Faculty of Law in Maastricht University. The speakers at this workshop included several professors and lawyers from the Netherlands, Germany, Belgium and China, and the author benefited a lot from their presentations and comments.

4 Innovation

Although there exists a number of reports, research papers and publications which study hosting ISPs' responsibilities for copyright infringement on their platforms, these research studies have not taken a comparative approach to comprehensively study the responsibility rules in the US, EU and China. In addition, the "safe harbor" provisions which regulate hosting ISPs' copyright responsibilities in the US, EU and China are per se homogenous, but the courts in these jurisdictions interpret these homogenous rules in different ways. This study examines at length the relevant case law in the US, EU and China, and compares how the courts in these jurisdictions interpret the norms set in "safe harbor" provisions. Besides finding out the differences between case laws, this study also contributes to analyzing how these differences affect the freedom to operate of hosting ISPs. Moreover, based on the comparison, this study concludes how the norms in "safe harbor" provisions ought to be interpreted so as to preserve maximum freedom for hosting ISPs to operate in the US, EU and China.

In addition, this study does not stop by examining the traditional legal norms, and also contributes to exploring the self-regulation agreements reached between copyright owners and hosting ISPs. In order to solve copyright disputes on hosting platforms, a number of self-regulation agreements have been reached. This study examines self-regulation norms by comparing them with traditional legal norms, and then draws the advantages and disadvantages of self-regulation in respect of preserving the freedom to operate of hosting ISPs. Moreover, this study also provides several recommendations for these hosting ISPs who are currently operating or planning to operate in the US, EU and China.

5 Planning and Implementation

How to regulate hosting ISPs' responsibilities is still an ongoing issue that attracts the attention of academics and practitioners, so there are many seminars, workshops and conferences which discuss this issue each year. In the past years, the author joined several workshops which focused on discussing the liability of online intermediaries, and got much useful feedback from experts during the discussions with them. Therefore, the author plans to present the results of study in different seminars, workshops and conferences. By doing so, the results of the study can be better spread, and the author can also obtain comments or even critiques from other experts, which can contribute to improving the author's research.

The author plans to translate parts of this study into Chinese and get them published in Chinese journals. When China drafted its own "safe harbor" provisions, the legislators in China took DMCA § 512 and E-commerce Directive as two important references. The academics and practitioners in China should be quite interested to read this study, especially the parts about how the courts in the US and EU interpret the norms set in "safe harbor" provisions, and then learn a lesson from the case law in the US and EU.

The author also plans to refine Chapters 5 and 6 of this thesis, and then publish them in English journals. These two chapters are the study results of two research projects that the author was engaged in. They take a comparative approach to study the notice-and-takedown procedures and identity disclosure mechanisms in the US, EU and China. The author believes that after refining, these two chapters can be accepted by the journals which are interested in publishing comparative study.

The Internet has become an important way for the public to access the information they need, so the author plans to publish parts of this study on the Internet. The Center for Internet and Society in Stanford University has been running a project called World Intermediary Liability Map (WILMap), which invited both academics and practitioners from the world to draw an intermediary liability map of their own jurisdictions. This study makes a comprehensive analysis about hosting ISPs' copyright responsibilities in China, and the WILMap is a perfect platform to publish this research. The author has already contributed several case decisions to the Chinese webpage and will continue to send other parts of the study to WILMap in the future.